



## **Cisco MWR 2941 Mobile Wireless Edge Router Software Configuration Guide, Release 12.2(33)MRB**

September 2010

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relation between Cisco and any other company. (1005R)

*Cisco MWR 2941 Mobile Wireless Edge Router Software Configuration Guide, Release 12.2(33)MRB*

Copyright © 2010, Cisco Systems, Inc.

All rights reserved. Printed in USA.



## CONTENTS

### About This Guide ix

Document Revision History ix

Objectives ix

Audience x

Organization x

Conventions x

Related Documentation xi

Obtaining Documentation, Obtaining Support, and Security Guidelines xii

## CHAPTER 1

### Cisco MWR 2941 Router Overview 1-1

Introduction 1-2

RAN Transport Solutions 1-2

Features 1-3

Cisco Pseudowire Emulation Edge-to-Edge 1-3

Structure-agnostic TDM over Packet 1-3

Structure-aware TDM Circuit Emulation Service over Packet-Switched Network 1-4

Transportation of Service Using ATM over MPLS 1-4

Transportation of Service Using Ethernet over MPLS 1-4

Generic Routing Encapsulation (GRE) Tunneling 1-5

Resilient Ethernet Protocol (REP) 1-5

Ethernet Operations, Administration, and Maintenance (OAM) 1-10

Overview 1-10

Link OAM 1-11

Ethernet Connectivity Fault Management (CFM) 1-14

Ethernet Local Management Interface (E-LMI) 1-14

Clocking and Timing 1-14

Network Clocking Overview 1-14

Precision Timing Protocol (PTP) 1-15

Pseudowire-based Clocking 1-16

Synchronous Ethernet 1-16

Network Clock Quality Selection using REP 1-17

Routing Protocols 1-17

Bidirectional Forwarding Detection 1-17

Multicast Routing 1-18

Role of IP Multicast in Information Delivery	1-18
Multicast Group Transmission Scheme	1-18
IP Multicast Group Addressing	1-20
IP Multicast Address Scoping	1-21
Layer 2 Multicast Addresses	1-22
IP Multicast Delivery Modes	1-22
Protocol Independent Multicast	1-23
Multicast Group Modes	1-24
Rendezvous Points	1-25
Multicast Forwarding	1-28
MLPPP Optimization Features	1-32
Distributed Multilink Point-to-Point Protocol (dMLPPP) Offload	1-32
Layer 3 Virtual Private Networks	1-33
Intelligent Cell Site IP Services	1-33
Cell Site Points-of-Presence	1-33
Quality of Service	1-34
Traffic Classification	1-35
Traffic Marking	1-35
Traffic Queuing	1-35
Traffic Shaping	1-35
Network Management Features	1-35
Cisco Mobile Wireless Transport Manager (MWTM)	1-35
Cisco Active Network Abstraction (ANA)	1-36
SNMP MIB Support	1-36
Cisco Networking Services (CNS)	1-36
Limitations and Restrictions	1-36
Hardware Limitations and Restrictions	1-36
Software Limitations and Restrictions	1-37

## CHAPTER 2

### Cisco IOS Software Basics 2-1

Getting Help	2-1
Understanding Command Modes	2-2
Undoing a Command or Feature	2-3
Saving Configuration Changes	2-3

## CHAPTER 3

### First-Time Configuration 3-1

Understanding the Cisco MWR 2941 Router Interface Numbering	3-1
Slot and Port Numbering	3-2
Setup Command Facility	3-3

Before Starting Your Router	3-3
Using the Setup Command Facility	3-4
Configuring Global Parameters	3-4
Completing the Configuration	3-6

**CHAPTER 4****Configuring the Cisco MWR 2941 Router Using the CLI 4-1**

Verifying the Cisco IOS Software Version	4-1
Configuration Sequence	4-1
Summary of Steps	4-2
Configuring the Hostname and Password	4-2
Verifying the Hostname and Password	4-3
Configuring Gigabit Ethernet Interfaces	4-4
Configuring the Interface Properties	4-4
Setting the Speed and Duplex Mode	4-5
Enabling the Interface	4-6
Creating Backup Switch Interfaces	4-6
Configuring Layer 2 Interfaces	4-6
Configuring a Range of Interfaces	4-6
Defining a Range Macro	4-7
Configuring Layer 2 Optional Interface Features	4-7
Configuring HWIC-9ESW Interfaces	4-11
Configuring Stacking	4-11
Configuring VLANs	4-12
Adding a VLAN Instance	4-12
Deleting a VLAN Instance	4-12
Configuring VLAN Trunking Protocol	4-13
Configuring Resilient Ethernet Protocol (REP)	4-15
Default REP Configuration	4-15
REP Configuration Guidelines	4-15
Configuring the REP Administrative VLAN	4-16
Configuring REP Interfaces	4-17
Setting Manual Preemption for VLAN Load Balancing	4-19
Configuring SNMP Traps for REP	4-19
Monitoring REP	4-20
Configuring Ethernet Connectivity Fault Management (CFM)	4-21
Understanding Ethernet CFM	4-21
Configuring Ethernet CFM	4-30
Configuring Ethernet Link Operations, Administration, and Maintenance (OAM)	4-33
Enabling Ethernet OAM on an Interface	4-33

Stopping and Starting Link Monitoring Operations	4-34
Configuring Link Monitoring Options	4-34
Configuring Global Ethernet OAM Options Using a Template	4-35
Configuring a Port for RFI Support	4-37
Configuring Ethernet Local Management Interface (E-LMI)	4-38
Enabling Ethernet LMI on All Supported Interfaces	4-38
Enabling Ethernet LMI on a Single Supported Interface	4-38
Configuring Clocking and Timing	4-39
Configuring PTP Clocking	4-39
Configuring Pseudowire-based Clocking with Adaptive Clock Recovery	4-45
Configuring Synchronous Ethernet	4-47
Configuring Network Clock Quality Selection Using REP	4-47
Verifying Clock-related Settings	4-49
Configuring MLPPP Backhaul	4-49
Configuring the Card Type	4-49
Configuring E1 Controllers	4-50
Configuring T1 Controllers	4-52
Configuring ATM IMA	4-53
Configuring a Multilink Backhaul Interface	4-54
Configuring Multiprotocol Label Switching (MPLS)	4-58
Configuring Routing Protocols	4-59
Configuring BFD	4-59
Configuring BFD for OSPF	4-59
Configuring BFD for BGP	4-61
Configuring BFD for IS-IS	4-61
Configuring BFD for Static Routes	4-63
Configuring IP Multicast	4-64
Configuring Multicast in Sparse Mode with a Static Rendezvous Point	4-64
Configuring Source-Specific Multicast	4-66
Configuring Source Specific Multicast Mapping	4-68
Configuring Multicast VPN	4-71
Verifying a Multicast Configuration	4-73
Configuring Pseudowire	4-73
Using Pseudowire Classes	4-74
Using CEM Classes	4-75
Configuring GRE Tunneling	4-76
Using Pseudowire Labels	4-77
Configuring a Backup Peer	4-78
Configuring Structure-Agnostic TDM over Packet (SAToP)	4-79
Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN)	4-79

Configuring Transportation of Service Using ATM over MPLS	4-80
Configuring Transportation of Service Using Ethernet over MPLS	4-87
Configuring Layer 3 Virtual Private Networks (VPNs)	4-88
Configuring Quality of Service (QoS)	4-88
QoS Limitations	4-88
Sample QoS Configuration	4-93
Configuring Classification	4-95
Configuring Marking	4-97
Configuring Congestion Management	4-101
Configuring Shaping	4-103
Configuring Ethernet Trusted Mode	4-104
Configuring Link Noise Monitor	4-104
Usage Notes	4-106
Saving Configuration Changes	4-107
Monitoring and Managing the Cisco MWR 2941 Router	4-107
Using Cisco Mobile Wireless Transport Manager (MWTM)	4-107
Configuring SNMP Support	4-108
Enabling Remote Network Management	4-112
Show Commands for Monitoring the Cisco MWR 2941 Router	4-113
Configuring Cisco Networking Services (CNS)	4-115
Process Overview	4-116
Configuring a DHCP Server	4-116
Configuring a TFTP Server	4-117
Configuring the Cisco Configuration Engine	4-117
Verifying the Configuration	4-118

## APPENDIX A

### Sample Configurations A-1

Sample Configurations	A-1
Pseudowire Configurations	A-2
Asymmetric Pseudowire Configuration	A-2
Pseudowire Redundancy Configuration	A-10
TDM over MPLS Configuration	A-14
ATM over MPLS Configuration	A-17
Ethernet over MPLS Configuration	A-23
GRE Tunneling Configurations	A-26
CESoPSN with GRE Tunnel Backhaul	A-26
ATM over MPLS AAL5 SDU Mode with GRE Backhaul	A-27
Routing Sample Configurations	A-27
OSPF with BFD	A-27

BGP with BFD	A-31
IS-IS with BFD	A-34
Multicast Sample Configurations	A-37
Sparse Mode with a Static Rendezvous Point	A-37
Source-Specific Multicast	A-37
PTP Sample Configurations	A-38
PTP Slave Mode with Redundancy	A-38
PTP Redundancy	A-43
PTP Hybrid Mode	A-44
PTP Hot Standby Master Clock	A-44
PTP Input Timing	A-45
PTP Output Timing	A-46
Layer 3 VPN Sample Configuration	A-46
QoS Sample Configurations	A-48
Switchport Priority	A-49
Classification and Marking	A-49
Priority Queuing	A-51
Resilient Ethernet Protocol (REP) Sample Configuration	A-51
Cisco Networking Services (CNS) Zero Touch Deployment Configuration	A-54
CFM and ELMI Sample Configuration	A-54

---

**APPENDIX B**

**Cisco MWR 2941 Router Command Reference B-1**

---

**INDEX**





## About This Guide

---

This section describes the objectives, audience, organization, and conventions of this software configuration guide. It contains the following sections:

- [Document Revision History, page ix](#)
- [Objectives, page ix](#)
- [Audience, page x](#)
- [Organization, page x](#)
- [Conventions, page x](#)
- [Related Documentation, page xi](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page xii](#)

## Document Revision History

The Document Revision History table below records technical changes to this document.

Document Number	Date	Change Summary
OL-21227-01	January 2010	Initial release for Release 12.2(33)MRA.
OL-21227-02	May 2010	Updated for Release 12.2(33)MRB.
OL-21227-02	September 2010	Updated for Release 12.2(33)MRB3.

## Objectives

This guide explains how to configure software features on the Cisco MWR 2941-DC and MWR 2941-DC-A routers. Unless otherwise stated, features described in this guide apply to both the Cisco MWR 2941-DC and the Cisco MWR 2941-DC-A.

# Audience

This publication is for the person responsible for configuring the router. This guide is intended for the following audiences:

- Customers with technical networking background and experience
- System administrators who are familiar with the fundamentals of router-based internetworking, but who may not be familiar with Cisco IOS software
- System administrators who are responsible for installing and configuring internetworking equipment, and who are familiar with Cisco IOS software

# Organization

The major sections of this software configuration guide are listed in the following table:

Chapter	Title	Description
Chapter 1	<a href="#">Cisco MWR 2941 Router Overview</a>	Describes the purpose of the Cisco MWR 2941 router and its unique software features.
Chapter 2	<a href="#">Cisco IOS Software Basics</a>	Describes what you need to know about the Cisco IOS software.
Chapter 3	<a href="#">First-Time Configuration</a>	Describes how to use the setup command facility to configure basic attributes of your router.
Chapter 4	<a href="#">Configuring the Cisco MWR 2941 Router Using the CLI</a>	Describes how to use the Cisco IOS software command-line interface (CLI) to configure basic router functionality.
Appendix A	<a href="#">Sample Configurations</a>	Provides examples of configurations.
Appendix B	<a href="#">Cisco MWR 2941 Router Command Reference</a>	Provides information about new and changed commands.
Index		

# Conventions

This publication uses the following conventions to convey instructions and information.

Convention	Description
<b>boldface font</b>	Commands and keywords.
<i>italic font</i>	Variables for which you supply values.
[    ]	Keywords or arguments that appear within square brackets are optional.
{ x   y   z }	A choice of required keywords appears in braces separated by vertical bars. You must select one.
screen font	Examples of information displayed on the screen.
<b>boldface screen font</b>	Examples of information the user enters.

Convention	Description
< >	Nonprinting characters, for example passwords, appear in angle brackets.
[ ]	Default responses to system prompts appear in square brackets.

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

**Tip**

Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

## Related Documentation

The following list includes documentation related to your product by implementation.

- Cisco MWR 2941 Mobile Wireless Edge Router Documents
  - *Cisco MWR 2941 Mobile Wireless Edge Router Hardware Installation Guide*
  - *Regulatory Compliance and Safety Information for the Cisco MWR 2941 Routers*
- Cisco Interface Cards Installation Guides
  - *Quick Start Guide: Interface Cards*
  - Cisco Interface Cards Installation Guide
- Release Notes
  - *Release Notes for Cisco MWR 2941 Mobile Wireless Edge Router for Cisco IOS Release 12.2(33)MRB*

**Note**

To obtain the latest information, access the online documentation.

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>



# CHAPTER 1

## Cisco MWR 2941 Router Overview

---

The Cisco MWR 2941 Mobile Wireless Router is cell-site access platforms specifically designed to aggregate and transport mixed-generation radio access network (RAN) traffic. The router is used at the cell site edge as a part of a 2G, 3G, or 4G radio access network (RAN). The Cisco MWR 2941 includes the following models:

- Cisco MWR 2941-DC
- Cisco MWR 2941-DC-A

The Cisco MWR 2941 router helps enable a variety of RAN solutions by extending IP connectivity to devices using Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), Node Bs using HSPA or LTE, base transceiver stations (BTSs) using Enhanced Data Rates for GSM Evolution (EDGE), Code Division Multiple Access (CDMA), CDMA-2000, EVDO, or WiMAX, and other cell-site equipment. It transparently and efficiently transports cell-site voice, data, and signaling traffic over IP using traditional T1/E1 circuits, including leased line, microwave, and satellite, as well as alternative backhaul networks, including Carrier Ethernet, DSL, Ethernet in the First Mile (EFM), and WiMAX. It also supports standards-based Internet Engineering Task Force (IETF) Internet protocols over the RAN transport network, including those standardized at the Third-Generation Partnership Project (3GPP) for IP RAN transport.

Custom designed for the cell site, the Cisco MWR 2941 features a small form factor, extended operating temperature, and cell-site DC input voltages.



### Note

The Cisco MWR 2941-DC and 2941-DC-A support the same features except for commands related to the 1PPS, 10Mhz, 2.048Mhz, and 1.544Mhz timing ports that are included on the 2941-DC-A. For more information, see the *Release Notes for Cisco MWR 2941-DC Mobile Wireless Edge Router for Cisco IOS Release 12.2(33)MRB*.

---

This chapter includes the following sections:

- [Introduction, page 1-2](#)
- [Features, page 1-3](#)
- [Network Management Features, page 1-35](#)
- [Limitations and Restrictions, page 1-36](#)

# Introduction

A typical RAN is composed of thousands of base transceiver stations (BTSs)/Node Bs, hundreds of base station controllers/radio network controllers (BSCs/RNCs), and several mobile switching centers (MSCs). The BTS/Node Bs and BSC/RNC are often separated by large geographic distances, with the BTSs/Node Bs located in cell sites uniformly distributed throughout a region, and the BSCs, RNCs, and MSCs located at suitably chosen Central Offices (CO) or mobile telephone switching offices (MTSO).

The traffic generated by a BTS/Node B is transported to the corresponding BSC/RNC across a network, referred to as the backhaul network, which is often a hub-and-spoke topology with hundreds of BTS/Node Bs connected to a BSC/RNC by point-to-point time division multiplexing (TDM) trunks. These TDM trunks may be leased-line T1/E1s or their logical equivalents, such as microwave links or satellite channels.

## RAN Transport Solutions

The Cisco MWR 2941 Mobile Wireless Router supports a variety of RAN transport solutions, including the following:

- IP/Multiprotocol Label Switching (MPLS) RAN backhaul: Allows you to create a high-speed backhaul for a variety of traffic types, including GSM, CDMA, HSPA/LTE, CDMA, EVDO, and WiMAX networks.
- Cell-site operations support networks: Facilitates telemetry to cell sites for remote operations and network element management.
- Cell-site IP points of presence (POPs): Allows you to offer IP services and applications at cell sites.
- Carrier Ethernet features including Resilient Ethernet Protocol (REP), Ethernet Connectivity Fault Management (CFM), Ethernet Local Management Interface (E-LMI), and Ethernet Operations, Administration, and Maintenance (OAM).
- Network clocking features including PTP, pseudowire-based clocking, and synchronous Ethernet.
- Flexible backhaul transport including MLPPP over T1, E1, xDSL, and Ethernet.

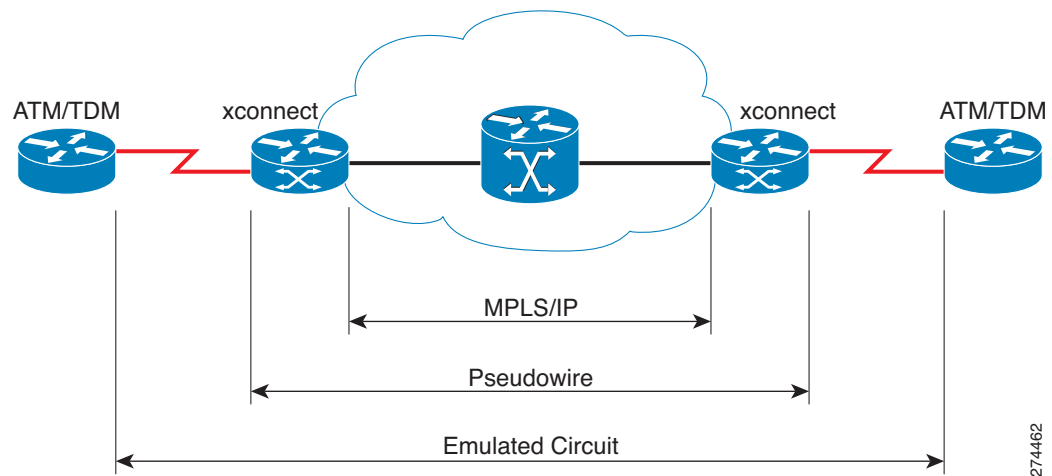
# Features

The following sections describe the features available in the Cisco MWR 2941 router.

## Cisco Pseudowire Emulation Edge-to-Edge

Cisco Pseudowire Emulation Edge-to-Edge (PWE3) allows you to transport traffic using traditional services such as E1/T1 over a packet-based backhaul technology such as MPLS or IP. A pseudowire (PW) consists of a connection between two provider edge (PE) devices that connects two attachment circuits (ACs), such as ATM VPIs/VCIs or E1/T1 links. [Figure 1-1](#) shows a sample pseudowire topology.

**Figure 1-1** Cisco MWR 2941 Router in a PWE3—Example



PWs manage encapsulation, timing, order, and other operations in order to make it transparent to users; the PW tunnel appears as an unshared link or circuit of the emulated service.

There are limitations that impede some applications from utilizing a PW connection. For more information, see the section describing the PW service.

Cisco supports the following standards-based PWE types:

- [Structure-agnostic TDM over Packet, page 1-3](#)
- [Structure-aware TDM Circuit Emulation Service over Packet-Switched Network, page 1-4](#)
- [Transportation of Service Using ATM over MPLS, page 1-4](#)
- [Transportation of Service Using Ethernet over MPLS, page 1-4](#)

## Structure-agnostic TDM over Packet

SAToP encapsulates TDM bit-streams (T1, E1, T3, E3) as PWs over PSNs. It disregards any structure that may be imposed on streams, in particular the structure imposed by the standard TDM framing.

The protocol used for emulation of these services does not depend on the method in which attachment circuits are delivered to the PEs. For example, a T1 attachment circuit is treated the same way for all delivery methods, including: PE on copper, multiplex in a T3 circuit, mapped into a virtual tributary of

a SONET/SDH circuit, or carried over a network using unstructured Circuit Emulation Service (CES). Termination of specific carrier layers used between the PE and circuit emulation (CE) is performed by an appropriate network service provider (NSP).

For instructions on how to configure SAToP, see the [“Configuring Structure-Agnostic TDM over Packet \(SAToP\)” section on page 4-79](#). For a sample SAToP configuration, see the [“TDM over MPLS Configuration” section on page A-14](#).

## Structure-aware TDM Circuit Emulation Service over Packet-Switched Network

CESoPSN encapsulates structured (NxDS0) TDM signals as PWs over PSNs. It complements similar work for structure-agnostic emulation of TDM bit-streams, such as PWE3-SAToP.

Emulation of NxDS0 circuits saves PSN bandwidth and supports DS0-level grooming and distributed cross-connect applications. It also enhances resilience of CE devices due to the effects of loss of packets in the PSN.

CESoPSN supports channel-associated signaling (CAS) for E1 and T1 interfaces. CAS provides signaling information within each DS0 channel as opposed to using a separate signaling channel. CAS also referred to as in-band signaling or robbed bit signaling.

For instructions on how to configure SAToP, see the [“Configuring Circuit Emulation Service over Packet-Switched Network \(CESoPSN\)” section on page 4-79](#). For a sample SAToP configuration, see the [“TDM over MPLS Configuration” section on page A-14](#).

## Transportation of Service Using ATM over MPLS

An Asynchronous Transfer Mode (ATM) over MPLS PW is used to carry ATM cells over an MPLS network. It is an evolutionary technology that allows you to migrate packet networks from legacy networks, yet provides transport for legacy applications. ATM over MPLS is particularly useful for transporting 3G voice traffic over MPLS networks.

You can configure ATM over MPLS in the following modes:

- N-to-1 Cell Mode—Maps one or more ATM virtual channel connections (VCCs) or virtual permanent connection (VPCs) to a single pseudowire.
- 1-to-1 Cell Mode—Maps a single ATM VCC or VPC to a single pseudowire.
- Port Mode—Map one physical port to a single pseudowire connection.

The Cisco MWR 2941 also supports cell packing and PVC mapping for ATM over MPLS pseudowires.

For more information about how to configure ATM over MPLS, see the [“Configuring Transportation of Service Using ATM over MPLS” section on page 4-80](#). For sample ATM over MPLS configurations, see the [“ATM over MPLS Configuration” section on page A-17](#).

## Transportation of Service Using Ethernet over MPLS

Ethernet over MPLS (EoMPLS) PWs provide a tunneling mechanism for Ethernet traffic through an MPLS-enabled Layer 3 core network. EoMPLS PWs encapsulate Ethernet protocol data units (PDUs) inside MPLS packets and use label switching to forward them across an MPLS network. EoMPLS PWs are an evolutionary technology that allows you to migrate packet networks from legacy networks while providing transport for legacy applications. EoMPLS PWs also simplify provisioning, since the provider edge equipment only requires Layer 2 connectivity to the connected customer edge (CE) equipment. The Cisco MWR 2941 implementation of EoMPLS PWs is compliant with the RFC 4447 and 4448 standards.



For instructions on how to create an EoMPLS PW, see the [“Configuring Transportation of Service Using Ethernet over MPLS”](#) section on page 4-87.

## Limitations

When configuring an EoMPLS pseudowire on the Cisco MWR 2941, you cannot configure an IP address on the same interface as the pseudowire.

## Generic Routing Encapsulation (GRE) Tunneling

Generic routing encapsulation (GRE) is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. GRE tunneling allows you to transport a pseudowire over an IP backhaul network when MPLS routing is not available between a cell site (BTS or Node-B) and an aggregation point (BSC or RNC). The Cisco MWR 2941 supports GRE encapsulation for the following PW connection types:

- ATM over MPLS
- SAToP
- CESoPSN
- Ethernet over MPLS

The Cisco MWR 2941 implementation of GRE can interoperate with the Cisco 7600 router and provides compliance with RFCs 2784 and 4023. The Cisco MWR 2941 supports up to 128 GRE tunnels. For more information about how to configure GRE tunneling, see the [“Configuring GRE Tunneling”](#) section on page 4-76.

## Resilient Ethernet Protocol (REP)

A REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (nonedge) segment ports and two user-configured edge ports. A switch can have only two ports belonging to the same segment, and each segment port can have only one external neighbor. A segment can go through a shared medium, but on any link, only two ports can belong to the same segment. REP is supported only on Layer 2 trunk interfaces.

[Figure 1-2](#) shows an example of a segment consisting of six ports spread across four switches. Ports E1 and E2 are configured as edge ports. When all ports are operational (as in the segment on the left), a single port is blocked, shown by the diagonal line. When there is a network failure, as shown in the diagram on the right, the blocked port returns to the forwarding state to minimize network disruption.

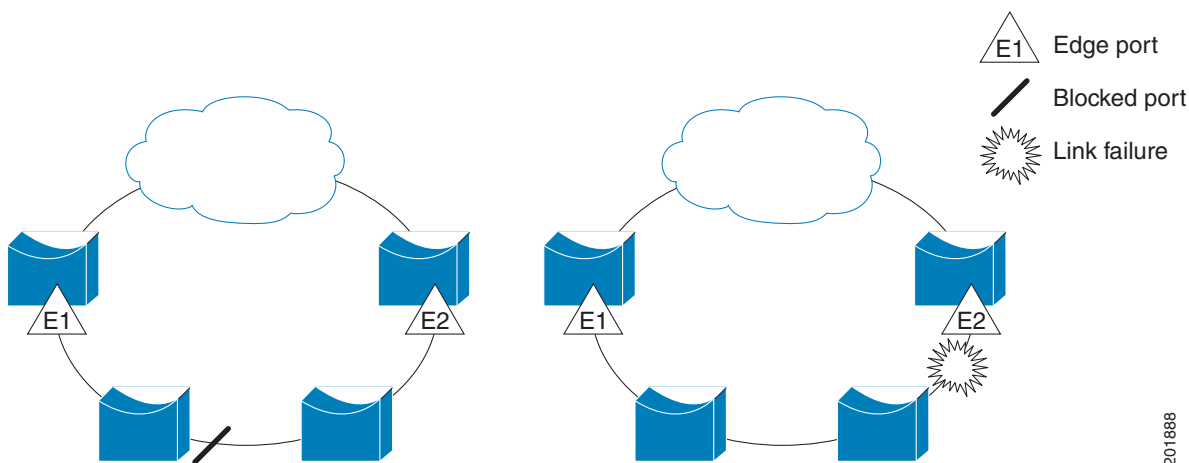
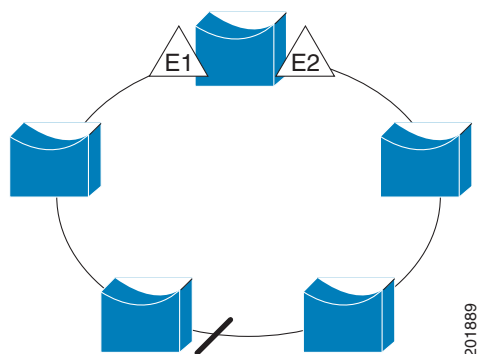
**Figure 1-2 REP Open Segments**

Figure 1-2 shows an open segment; there is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop, and you can safely connect the segment edges to any network. All hosts connected to switches inside the segment have two possible connections to the rest of the network through the edge ports, but only one connection is accessible at any time. If a host cannot access its usual gateway because of a failure, REP unblocks all ports to ensure that connectivity is available through the other gateway.

Figure 1-3 shows a segment with both edge ports located on the same switch, is a ring segment. In this configuration, there is connectivity between the edge ports through the segment. With this configuration, you can create a redundant connection between any two switches in the segment.

**Figure 1-3 REP Ring Segment**

REP segments have these characteristics:

- If all ports in the segment are operational, one port (referred to as the *alternate* port) is in the blocked state for each VLAN.
- If VLAN load balancing is configured, two ports in the segment control the blocked state of VLANs.
- If one or more ports in a segment is not operational, causing a link failure, all ports forward traffic on all VLANs to ensure connectivity.
- In case of a link failure, the alternate ports are unblocked as quickly as possible. When the failed link comes back up, a logically blocked port per VLAN is selected with minimal disruption to the network.

You can construct almost any type of network based on REP segments. REP also supports VLAN load-balancing, controlled by the primary edge port but occurring at any port in the segment.

REP has these limitations:

- You must configure each segment port; an incorrect configuration can cause forwarding loops in the networks.
- REP can manage only a single failed port within the segment; multiple port failures within the REP segment cause loss of network connectivity.
- You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

## Link Integrity

REP does not use an end-to-end polling mechanism between edge ports to verify link integrity. It implements local link failure detection. The REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. All VLANs are blocked on an interface until it detects the neighbor. After the neighbor is identified, REP determines which neighbor port should become the alternate port and which ports should forward traffic.

Each port in a segment has a unique port ID. The port ID format is similar to that used by the spanning tree algorithm: a port number (unique on the bridge), associated to a MAC address (unique in the network). When a segment port is coming up, its LSL starts sending packets that include the segment ID and the port ID. The port is declared operational after it performs a three-way handshake with a neighbor in the same segment.

A segment port does not become operational if:

- No neighbor has the same segment ID.
- More than one neighbor has the same segment ID.
- The neighbor does not acknowledge the local port as a peer.

Each port creates an adjacency with its immediate neighbor. After the neighbor adjacencies are created, the ports negotiate to determine one blocked port for the segment, the alternate port. All other ports become unblocked. By default, REP packets are sent to a BPDU class MAC address. The packets can also be sent to the Cisco multicast address, which is used only to send blocked port advertisement (BPA) messages when there is a failure in the segment. The packets are dropped by devices not running REP.

## Fast Convergence

Because REP runs on a physical link basis and not on a per-VLAN basis, only one hello message is required for all VLANs, reducing the load on the protocol. We recommend that you create VLANs consistently on all switches in a given segment and configure the same allowed VLANs on the REP trunk ports. To avoid the delay introduced by relaying messages in software, REP also allows some packets to be flooded to a regular multicast address. These messages operate at the hardware flood layer (HFL) and are flooded to the whole network, not just the REP segment. Switches that do not belong to the segment treat them as data traffic. You can control flooding of these messages by configuring a dedicated administrative VLAN for the whole domain.

The estimated convergence recovery time on fiber interfaces is less than 200 ms for the local segment with 200 VLANs configured. Convergence for VLAN load balancing is 300 ms or less.

## VLAN Load Balancing

One edge port in the REP segment acts as the primary edge port; the other as the secondary edge port. The primary edge port always participates in VLAN load balancing in the segment. REP VLAN balancing is achieved by blocking some VLANs at a configured alternate port and all other VLANs at the primary edge port. When you configure VLAN load balancing, you can specify the alternate port in one of three ways:

- Enter the port ID of the interface. To identify the port ID of a port in the segment, enter the **show interface rep detail** interface configuration command for the port.
- Enter the neighbor offset number of a port in the segment, which identifies the downstream neighbor port of an edge port. The neighbor offset number range is -256 to +256; a value of 0 is invalid. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors.

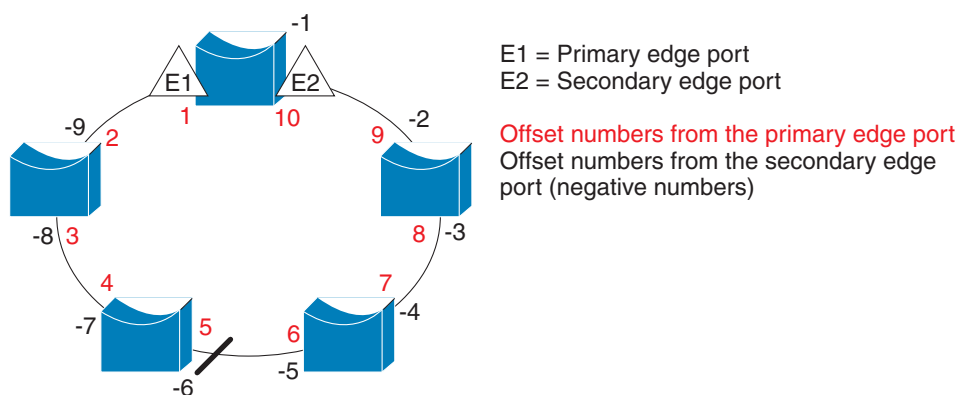


**Note** You configure offset numbers on the primary edge port by identifying the downstream position from the primary (or secondary) edge port. You would never enter an offset value of 1 because that is the offset number of the primary edge port itself.

Figure 1-4 shows neighbor offset numbers for a segment where E1 is the primary edge port and E2 is the secondary edge port. The red numbers inside the ring are numbers offset from the primary edge port; the black numbers outside the ring show the offset numbers from the secondary edge port. Note that you can identify all ports (except the primary edge port) by either a positive offset number (downstream position from the primary edge port) or a negative offset number (downstream position from the secondary edge port). If E2 became the primary edge port, its offset number would then be 1, and E1 would be -1.

- By entering the **preferred** keyword to select the port that you previously configured as the preferred alternate port with the **rep segment segment-id preferred** command in interface configuration mode.

**Figure 1-4 Neighbor Offset Numbers in a Segment**



When the REP segment is complete, all VLANs are blocked. When you configure VLAN load balancing, you must also configure triggers in one of two ways

- Manually trigger VLAN load balancing at any time by entering the **rep preempt segment segment-id** privileged EXEC command on the switch that has the primary edge port.

- Configure a preempt delay time by entering the **rep preempt delay** *seconds* interface configuration command. After a link failure and recovery, VLAN load balancing begins after the configured preemption time period elapses. Note that the delay timer restarts if another port fails before the time has elapsed.

**Note**

When VLAN load balancing is configured, it does not start working until triggered by either manual intervention or a link failure and recovery.

When VLAN load balancing is triggered, the primary edge port sends a message to alert all interfaces in the segment about the preemption. When the secondary port receives the message, it is reflected into the network to notify the alternate port to block the set of VLANs specified in the message and to notify the primary edge port to block the remaining VLANs.

You can also configure a particular port in the segment to block all VLANs. Only the primary edge port initiates VLAN load balancing, which is not possible if the segment is not terminated by an edge port on each end. The primary edge port determines the local VLAN load balancing configuration.

Reconfigure the primary edge port to reconfigure load balancing. When you change the load balancing configuration, the primary edge port again waits for the **rep preempt segment** command or for the configured preempt delay period after a port failure and recovery before executing the new configuration. If you change an edge port to a regular segment port, the existing VLAN load balancing status does not change. Configuring a new edge port might cause a new topology configuration.

## Spanning Tree Interaction

REP does not interact with STP or with the Flex Link feature, but can coexist with both. A port that belongs to a segment is removed from spanning tree control and STP BPDUs are not accepted or sent from segment ports.

To migrate from an STP ring configuration to REP segment configuration, begin by configuring a single port in the ring as part of the segment, and continue by configuring contiguous ports to minimize the number of segments. Each segment always contains a blocked port, so multiple segments means multiple blocked ports and a potential loss of connectivity. When the segment has been configured in both directions to the edge ports, you then configure the edge ports.

## REP Ports

Ports in REP segments are Failed, Open, or Alternate.

- A port configured as a regular segment port starts as a failed port.
- After the neighbor adjacencies are determined, the port changes to alternate port state, blocking all VLANs on the interface. Blocked port negotiations occur and when the segment settles, one blocked port remains in the alternate role, and all other ports become open ports.
- When a failure occurs in a link, all ports move to the open state. When the alternate port receives the failure notification, it changes to the open state, forwarding all VLANs.

A regular segment port converted to an edge port, or an edge port converted to a regular segment port, does not always result in a topology change. If you convert an edge port into a regular segment port, VLAN load balancing is not implemented unless it has been configured. For VLAN load balancing, you must configure two edge ports in the segment.

A segment port that is reconfigured as a spanning tree port restarts according the spanning tree configuration. By default, this is a designated blocking port. If PortFast is configured or if STP is disabled, the port goes into the forwarding state.

For instructions on how to configure REP, see the [“Configuring Resilient Ethernet Protocol \(REP\)” section on page 4-15](#).

## Ethernet Operations, Administration, and Maintenance (OAM)

Ethernet Operations, Administration, and Maintenance (OAM) is a protocol for installing, monitoring, and troubleshooting Ethernet metropolitan-area networks (MANs) and Ethernet WANs. It relies on a new, optional sublayer in the data link layer of the Open Systems Interconnection (OSI) model. The OAM features covered by this protocol are Discovery, Link Monitoring, Remote Fault Detection, Remote Loopback, and Cisco Proprietary Extensions.

The following sections describe the Ethernet OAM features supported on the Cisco MWR 2941:

- [Overview](#)
- [Link OAM](#)
- [Ethernet Connectivity Fault Management \(CFM\)](#)
- [Ethernet Local Management Interface \(E-LMI\)](#)

### Overview

Ethernet OAM is a protocol for installing, monitoring, and troubleshooting metro Ethernet networks and Ethernet WANs. It relies on a new, optional sublayer in the data link layer of the OSI model. Ethernet OAM can be implemented on any full-duplex point-to-point or emulated point-to-point Ethernet link. A system-wide implementation is not required; OAM can be deployed on particular interfaces for part of a system.

Normal link operation does not require Ethernet OAM. OAM frames, called OAM protocol data units (PDUs), use the slow protocol destination MAC address 0180.c200.0002. They are intercepted by the MAC sublayer and cannot propagate beyond a single hop within an Ethernet network.

Ethernet OAM is a relatively slow protocol with modest bandwidth requirements. The frame transmission rate is limited to a maximum of 10 frames per second; therefore, the impact of OAM on normal operations is negligible. However, when link monitoring is enabled, the CPU must poll error counters frequently. In this case, the required CPU cycles will be proportional to the number of interfaces that have to be polled.

Two major components, the OAM client and the OAM sublayer, make up Ethernet OAM. The following sections describe these components.

### OAM Client

The OAM client is responsible for establishing and managing Ethernet OAM on a link. The OAM client also enables and configures the OAM sublayer. During the OAM discovery phase, the OAM client monitors OAM PDUs received from the remote peer and enables OAM functionality on the link based on local and remote state as well as configuration settings. Beyond the discovery phase (at steady state), the OAM client is responsible for managing the rules of response to OAM PDUs and managing the OAM remote loopback mode.

## OAM Sublayer

The OAM sublayer presents two standard IEEE 802.3 MAC service interfaces: one facing toward the superior sublayers, which include the MAC client (or link aggregation), and the other interface facing toward the subordinate MAC control sublayer. The OAM sublayer provides a dedicated interface for passing OAM control information and OAM PDUs to and from a client.

The OAM sublayer is made up of three components: control block, multiplexer, and packet parser (p-parser). Each component is described in the following sections.

### Control Block

The control block provides the interface between the OAM client and other blocks internal to the OAM sublayer. The control block incorporates the discovery process, which detects the existence and capabilities of remote OAM peers. It also includes the transmit process that governs the transmission of OAM PDUs to the multiplexer and a set of rules that govern the receipt of OAM PDUs from the p-parser.

### Multiplexer

The multiplexer manages frames generated (or relayed) from the MAC client, control block, and p-parser. The multiplexer passes through frames generated by the MAC client untouched. It passes OAM PDUs generated by the control block to the subordinate sublayer; for example, the MAC sublayer. Similarly, the multiplexer passes loopback frames from the p-parser to the same subordinate sublayer when the interface is in OAM remote loopback mode.

### P-Parser

The p-parser classifies frames as OAM PDUs, MAC client frames, or loopback frames and then dispatches each class to the appropriate entity. OAM PDUs are sent to the control block. MAC client frames are passed to the superior sublayer. Loopback frames are dispatched to the multiplexer.

## Link OAM

Link OAM is defined in the IEEE 802.3ah and IEEE 802.3 Clause 57 standards and provides for discovery, Link Monitoring, Remote Fault Indication, Remote Loopback, and Cisco proprietary extensions. The following sections describe Link OAM:

- [Discovery](#)
- [Link Monitoring](#)
- [Remote Failure Indication](#)
- [Remote Loopback](#)
- [Cisco Vendor-Specific Extensions](#)
- [OAM Messages](#)

## Discovery

Discovery is the first phase of Ethernet OAM and it identifies the devices in the network and their OAM capabilities. Discovery uses information OAM PDUs. During the discovery phase, the following information is advertised within periodic information OAM PDUs:

- OAM mode—Conveyed to the remote OAM entity. The mode can be either active or passive and can be used to determine device functionality.

- OAM configuration (capabilities)—Advertises the capabilities of the local OAM entity. With this information a peer can determine what functions are supported and accessible; for example, loopback capability.
- OAM PDU configuration—Includes the maximum OAM PDU size for receipt and delivery. This information along with the rate limiting of 10 frames per second can be used to limit the bandwidth allocated to OAM traffic.
- Platform identity—A combination of an organization unique identifier (OUI) and 32-bits of vendor-specific information. OUI allocation, controlled by the IEEE, is typically the first three bytes of a MAC address.

Discovery includes an optional phase in which the local station can accept or reject the configuration of the peer OAM entity. For example, a node may require that its partner support loopback capability to be accepted into the management network. These policy decisions may be implemented as vendor-specific extensions.

## Link Monitoring

Link monitoring in Ethernet OAM detects and indicates link faults under a variety of conditions. Link monitoring uses the event notification OAM PDU and sends events to the remote OAM entity when there are problems detected on the link. The error events include the following:

- Error Symbol Period (error symbols per second)—The number of symbol errors that occurred during a specified period exceeded a threshold. These errors are coding symbol errors.
- Error Frame (error frames per second)—The number of frame errors detected during a specified period exceeded a threshold.
- Error Frame Period (error frames per  $n$  frames)—The number of frame errors within the last  $n$  frames has exceeded a threshold.
- Error Frame Seconds Summary (error seconds per  $m$  seconds)—The number of error seconds (1-second intervals with at least one frame error) within the last  $m$  seconds has exceeded a threshold.

Because IEEE 802.3ah OAM does not provide a guaranteed delivery of any OAM PDU, the event notification OAM PDU may be sent multiple times to reduce the probability of a lost notification. A sequence number is used to recognize duplicate events.

## Remote Failure Indication

Faults in Ethernet connectivity that are caused by slowly deteriorating quality are difficult to detect. Ethernet OAM provides a mechanism for an OAM entity to convey these failure conditions to its peer via specific flags in the OAM PDU. The following failure conditions can be communicated:

- Link Fault—Loss of signal is detected by the receiver; for instance, the peer's laser is malfunctioning. A link fault is sent once per second in the information OAM PDU. Link fault applies only when the physical sublayer is capable of independently transmitting and receiving signals.
- Dying Gasp—An unrecoverable condition has occurred; for example, a power failure. This type of condition is vendor specific. A notification about the condition may be sent immediately and continuously.
- Critical Event—An unspecified critical event has occurred. This type of event is vendor specific. A critical event may be sent immediately and continuously.



## Remote Loopback

An OAM entity can put its remote peer into loopback mode using the loopback control OAM PDU. Loopback mode helps an administrator ensure the quality of links during installation or when troubleshooting. In loopback mode, every frame received is transmitted back on the same port except for OAM PDUs and pause frames. The periodic exchange of OAM PDUs must continue during the loopback state to maintain the OAM session.

The loopback command is acknowledged by responding with an information OAM PDU with the loopback state indicated in the state field. This acknowledgement allows an administrator, for example, to estimate if a network segment can satisfy a service-level agreement. Acknowledgement makes it possible to test delay, jitter, and throughput.

When an interface is set to the remote loopback mode the interface no longer participates in any other Layer 2 or Layer 3 protocols such as Spanning Tree Protocol (STP) or Open Shortest Path First (OSPF). The reason is that when two connected ports are in a loopback session, no frames other than the OAM PDUs are sent to the CPU for software processing. The non-OAM PDU frames are either looped back at the MAC level or discarded at the MAC level.

From a user's perspective, an interface in loopback mode is in a link-up state.

## Cisco Vendor-Specific Extensions

Ethernet OAM allows vendors to extend the protocol by allowing them to create their own type-length-value (TLV) fields.

## OAM Messages

Ethernet OAM messages or OAM PDUs are standard length, untagged Ethernet frames within the normal frame length bounds of 64 to 1518 bytes. The maximum OAM PDU frame size exchanged between two peers is negotiated during the discovery phase.

OAM PDUs always have the destination address of slow protocols (0180.c200.0002) and an Ethertype of 8809. OAM PDUs do not go beyond a single hop and have a hard-set maximum transmission rate of 10 OAM PDUs per second. Some OAM PDU types may be transmitted multiple times to increase the likelihood that they are successfully received on a deteriorating link.

Four types of OAM messages are supported:

- Information OAM PDU—A variable-length OAM PDU that is used for discovery. This OAM PDU includes local, remote, and organization-specific information.
- Event notification OAM PDU—A variable-length OAM PDU that is used for link monitoring. This type of OAM PDU may be transmitted multiple times to increase the chance of a successful receipt; for example, in the case of high-bit errors. Event notification OAM PDUs also may include a time stamp when generated.
- Loopback control OAM PDU—An OAM PDU fixed at 64 bytes in length that is used to enable or disable the remote loopback command.
- Vendor-specific OAM PDU—A variable-length OAM PDU that allows the addition of vendor-specific extensions to OAM.

For instructions on how to configure Ethernet Link OAM, see the [“Configuring Ethernet Link Operations, Administration, and Maintenance \(OAM\)”](#) section on page 4-33.

## Ethernet Connectivity Fault Management (CFM)

The Cisco MWR 2941 supports Ethernet Connectivity Fault Management (CFM) as defined in 802.1ag Draft 1.0. Ethernet Connectivity Fault Management (CFM) is an end-to-end per-service-instance Ethernet layer operations, administration, and maintenance (OAM) protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs.

Ethernet CFM provides the following benefits:

- End-to-end service-level OAM technology
- Reduced operating expense for service provider Ethernet networks
- Competitive advantage for service providers

**Note**

Release 12.2(33)MRA supports the Draft 1.0 version of Ethernet CFM; it does not support the IEEE 802.1ag-2007 version.

For instructions on how to configure CFM, see the [“Configuring Ethernet CFM” section on page 4-30](#).

## Ethernet Local Management Interface (E-LMI)

Ethernet Local Management Interface (LMI) is an Ethernet layer operation, administration, and management (OAM) protocol. It provides information that enables autoconfiguration of customer edge (CE) devices and provides the status of Ethernet virtual connections (EVCs) for large Ethernet metropolitan-area networks (MANs) and WANs. Specifically, Ethernet LMI notifies a CE device of the operating state of an EVC and the time when an EVC is added or deleted. Ethernet LMI also communicates the attributes of an EVC and a user-network interface (UNI) to a CE device.

For instructions on how to configure E-LMI, see the [“Configuring Ethernet Local Management Interface \(E-LMI\)” section on page 4-38](#).

## Clocking and Timing

The following sections describe the clocking and timing features available on the Cisco MWR 2941.

- [Network Clocking Overview](#)
- [Precision Timing Protocol \(PTP\)](#)
- [Pseudowire-based Clocking](#)
- [Synchronous Ethernet](#)

## Network Clocking Overview

Clock synchronization is important for a variety of applications, including synchronization of radio cell towers. While legacy TDM protocols incorporate timing features, packet-switched networks such as Ethernet do not natively include these features. The Cisco MWR 2941 supports legacy TDM technologies while supporting a variety of technologies that distribute clocking information over packet-switched networks.

Clocking is typically distributed from the core network outward to the BTS or Node B at the network edge. The Cisco MWR 2941 receives and transmits clocking information using any of the following ports:

- T1/E1
- Ethernet (GigabitEthernet and FastEthernet)
- DSL
- BITS/SYNC port
- 1PPS
- 1.544Mhz
- 2.048Mhz
- 10Mhz

## Precision Timing Protocol (PTP)

The Cisco MWR 2941 supports the Precision Time Protocol (PTP) as defined by the IEEE 1588-2008 standard. PTP provides for accurate time synchronization on over packet-switched networks. Nodes within a PTP network can act in one of the following roles:

- Grandmaster—A device on the network physically attached to the primary time source. All other clocks are ultimately synchronized to the grandmaster clock.
- Ordinary clock—An ordinary clock is a 1588 clock with a single PTP port that can serve in one of the following roles:
  - Master mode—Distributes timing information over the network to one or more slave clocks, thus allowing the slave to synchronize its clock to the master.
  - Slave mode—Synchronizes its clock to a master clock.
- Boundary clock—The device participates in selecting the best master clock and can act as the master clock if no better clocks are detected.
- Transparent clock—A device such as a switch that calculates the time it requires to forward traffic and updates the PTP time correction field to account for the delay, making the device transparent in terms of timing calculations.

**Note**

The Cisco MWR 2941 does not currently act as a boundary clock or a transparent clock.

**Note**

The 1588-2008 standard defines other clocking devices that are not described here.

## PTP Domains

PTP devices use a best master clock algorithm to determine the most accurate clock on a network and construct a clocking hierarchy based on the grandmaster clock. A given clocking hierarchy is called a PTP domain.

## Clock synchronization

PTP master devices periodically launch an exchange of messages with slave devices to help each slave clock recompute the offset between its clock and the master clock. Periodic clock synchronization mitigates any drift between the master and slave clocks.

## PTP Redundancy

The Cisco MWR 2941 supports the multicast- and unicast-based timing as specified in the 1588-2008 standard. The Cisco MWR 2941 can use multicast routing to establish redundant paths between an external PTP client and one or more PTP multicast master clocks.

When configured as a multicast PTP router, the Cisco MWR 2941 selects the best path toward a Rendezvous Point (RP) using the active routing protocol, sends a Cisco Protocol Independent Multicast (PIM) join message to the RP, and forwards PTP multicast messages to the PTP client. The Cisco MWR 2941 also supports PIM forwarding. For instructions on how to configure PTP redundancy using multicast, see the [“Configuring IP Multicast” section on page 4-64](#).

## Hot Standby Master Clock

The Cisco MWR 2941 supports a hot standby master clock for PTP clocking; the Cisco MWR 2941 selects the best clock source between two PTP master clocks and switches dynamically between them if the clock quality of the standby clock is greater than that of the current master clock. For instructions on how to configure a hot standby master clock, see the [“Configuring PTP Clocking” section on page 4-39](#).

## Hybrid Clocking

The Cisco MWR 2941 supports a hybrid clocking mode that uses clock frequency obtained from the synchronous Ethernet port while using phase (ToD or 1PPS) obtained using PTP. For instructions on how to configure hybrid clocking, see the [“Configuring PTP Clocking” section on page 4-39](#).

## Pseudowire-based Clocking

Pseudowire-based clocking allows the Cisco MWR 2941 router to

- Transmit and receive clocking information over a pseudowire interface
- Receive clocking over a virtual pseudowire interface.

The Cisco MWR 2941 can transmit clocking information within packet headers (in-band) or as a separate packet stream (out-of-band).

Pseudowire-based clocking also supports adaptive clock recovery (ACR), which allows the Cisco MWR 2941 to recover clocking from the headers of a packet stream. For instructions on how to configure pseudowire-based clocking, see the [“Configuring Clocking and Timing” section on page 4-39](#). For more information about using pseudowires, see the [“Cisco Pseudowire Emulation Edge-to-Edge” section on page 1-3](#).

## Synchronous Ethernet

Synchronous ethernet is a timing technology that allows the Cisco MWR 2941 to transport frequency and time information over Ethernet. Because frequency and time are embedded in Ethernet packets, synchronous Ethernet must be supported by each network element in the synchronization path. Synchronous Ethernet is defined in the ITU-T G.781, G.8261, G.8262, and G.8264, Telcordia GR-253-CORE, and Telcordia GR-1244-CORE standards.

You can use synchronous Ethernet in conjunction with an external timing technology such as GPS to synchronize timing across the network. For instructions on how to configure synchronous Ethernet, see the [“Configuring Clocking and Timing” section on page 4-39](#).

## Network Clock Quality Selection using REP

Ethernet Synchronization Message Channel (ESMC) is a method for indicating the quality of a clock source on a synchronous Ethernet network segment. ESMC is described in the G.8264 (2008) standard and is similar to the Synchronization Status Message (SSM) message used in SONET and SDH. ESMC is based on the Organization Specific Slow Protocol defined in the IEEE 802.3 standard.

Release 12.2(33)MRA provides support for ESMC for synchronous Ethernet segments using REP. Release 12.2(33)MRA does not provide support the G.8264 standard.

ESMC provides the following benefits:

- Quality level (QL) enabled implementation – Ensures the use of the highest available level of clock quality.
- Helps a node derive timing from most reliable source.
- Prevents timing loops.

For instructions on how to configure network clock quality selection using REP, see the [“Configuring Network Clock Quality Selection Using REP” section on page 4-47](#).

For more information about REP, see the [“Resilient Ethernet Protocol \(REP\)” section on page 1-5](#).

## Routing Protocols

In addition to static routing, the Cisco MWR 2941 supports the following dynamic routing protocols:

- OSPF—An Interior Gateway Protocol (IGP) designed expressly for IP networks that supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets.
- IS-IS—An Open System Interconnection (OSI) protocol that specifies how routers communicate with routers in different domains.
- BGP—An interdomain routing protocol designed to provide loop-free routing between separate routing domains that contain independent routing policies (autonomous systems).

For instructions on how to configure routing on the Cisco MWR 2941, see the [“Configuring Routing Protocols” section on page 4-59](#).

## Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent routers, including the interfaces, data links, and forwarding planes. BFD is a detection protocol that you enable at the interface and routing protocol levels. For instructions on how to configure BFD, see the [“Configuring BFD” section on page 4-59](#).

## Multicast Routing

The following sections describe the support for multicast routing on the Cisco MWR 2941.

- [Role of IP Multicast in Information Delivery](#)
- [Multicast Group Transmission Scheme](#)
- [IP Multicast Group Addressing](#)
- [IP Multicast Address Scoping](#)
- [Layer 2 Multicast Addresses](#)
- [IP Multicast Delivery Modes](#)
- [Protocol Independent Multicast](#)
- [Multicast Group Modes](#)
- [Rendezvous Points](#)
- [Multicast Forwarding](#)

### Role of IP Multicast in Information Delivery

IP multicast is a bandwidth-conserving technology that reduces traffic by delivering a single stream of information simultaneously to potentially thousands of businesses and homes. Applications that take advantage of multicast include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

IP multicast routing enables a host (source) to send packets to a group of hosts (receivers) anywhere within the IP network by using a special form of IP address called the IP multicast group address. The sending host inserts the multicast group address into the IP destination address field of the packet and IP multicast routers and multilayer switches forward incoming IP multicast packets out all interfaces that lead to the members of the multicast group. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message.

### Multicast Group Transmission Scheme

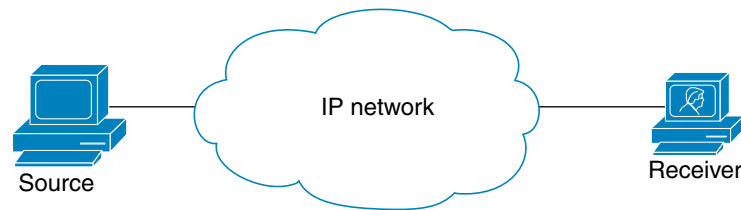
IP communication consists of hosts that act as senders and receivers of traffic as shown in [Figure 5](#). Senders are called sources. Traditional IP communication is accomplished by a single host source sending packets to another single host (*unicast transmission*) or to all hosts (*broadcast transmission*). IP multicast provides a third scheme, allowing a host to send packets to a subset of all hosts (*multicast transmission*). This subset of receiving hosts is called a multicast group. The hosts that belong to a multicast group are called group members.

Multicast is based on this group concept. A multicast group is an arbitrary number of receivers that join a group in order to receive a particular data stream. This multicast group has no physical or geographical boundaries—the hosts can be located anywhere on the Internet or on any private internetwork. Hosts that are interested in receiving data from a source to a particular group must join that group. Joining a group is accomplished by a host receiver by way of the Internet Group Management Protocol (IGMP).

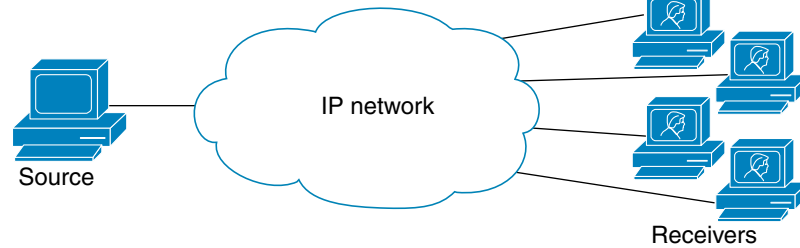
In a multicast environment, any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group can receive packets sent to that group. Multicast packets are delivered to a group using best-effort reliability, just like IP unicast packets.

**Figure 5 IP Transmission Schemes**

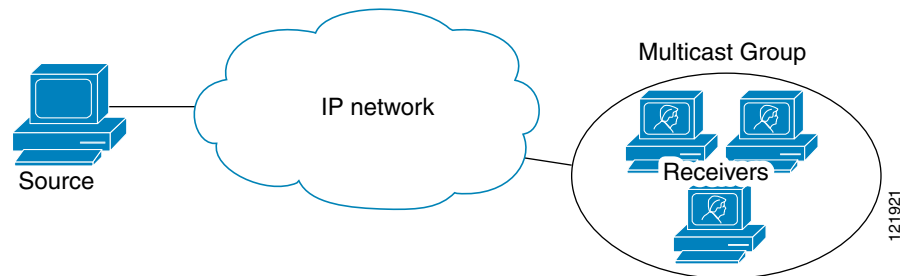
Unicast transmission—One host sends and the other receives.



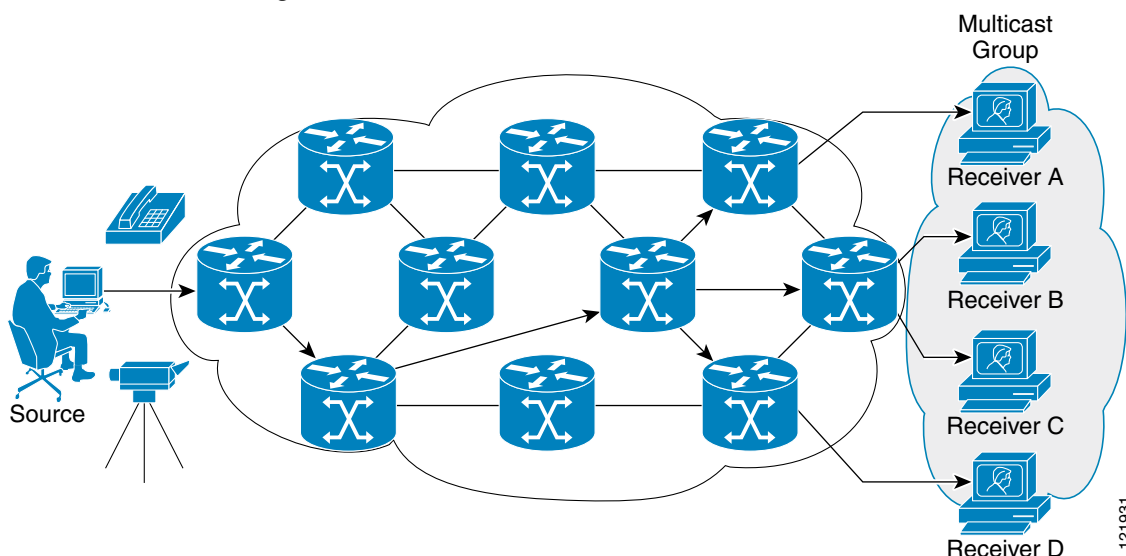
Broadcast transmission—One sender to all receivers.



Multicast transmission—One sender to a group of receivers.



In [Figure 6](#), the receivers (the designated multicast group) are interested in receiving the video data stream from the source. The receivers indicate their interest by sending an IGMP host report to the routers in the network. The routers are then responsible for delivering the data from the source to the receivers. The routers use Protocol Independent Multicast (PIM) (see the [“Protocol Independent Multicast” section on page 1-23](#)) to dynamically create a multicast distribution tree. The video data stream will then be delivered only to the network segments that are in the path between the source and the receivers.

**Figure 6 Multicast Transmission**

## IP Multicast Group Addressing

A multicast group is identified by its multicast group address. Multicast packets are delivered to that multicast group address. Unlike unicast addresses that uniquely identify a single host, multicast IP addresses do not identify a particular host. To receive the data sent to a multicast address, a host must join the group that address identifies. The data is sent to the multicast address and received by all the hosts that have joined the group indicating that they wish to receive traffic sent to that group. The multicast group address is assigned to a group at the source. Network administrators who assign multicast group addresses must make sure the addresses conform to the multicast address range assignments reserved by the Internet Assigned Numbers Authority (IANA).

## IP Class D Addresses

IP multicast addresses have been assigned to the IPv4 Class D address space by IANA. The high-order four bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 to 239.255.255.255. A multicast address is chosen at the source (sender) for the receivers in a multicast group.



### Note

The Class D address range is used only for the group address or destination address of IP multicast traffic. The source address for multicast datagrams is always the unicast source address.



## IP Multicast Address Scoping

The multicast address range is subdivided to provide predictable behavior for various address ranges and for address reuse within smaller domains. [Table 1](#) is a summary of the multicast address ranges. A brief summary description of each range follows.

**Table 1** *Multicast Address Range Assignments*

Name	Range	Description
Reserved Link-Local Addresses	224.0.0.0 to 224.0.0.255	Reserved for use by network protocols on a local network segment.
Globally Scoped Addresses	224.0.1.0 to 238.255.255.255	Reserved to send multicast data between organizations and across the Internet.
Source Specific Multicast	232.0.0.0 to 232.255.255.255	Reserved for use with the SSM datagram delivery model where data is forwarded only to receivers that have explicitly joined the group.
GLOP Addresses	233.0.0.0 to 233.255.255.255	Reserved for statically defined addresses by organizations that already have an assigned autonomous system (AS) domain number.
Limited Scope Address	239.0.0.0 to 239.255.255.255	Reserved as administratively or limited scope addresses for use in private multicast domains.

### Reserved Link-Local Addresses

The IANA has reserved the range 224.0.0.0 to 224.0.0.255 for use by network protocols on a local network segment. Packets with an address in this range are local in scope and are not forwarded by IP routers. Packets with link local destination addresses are typically sent with a time-to-live (TTL) value of 1 and are not forwarded by a router.

Within this range, reserved link-local addresses provide network protocol functions for which they are reserved. Network protocols use these addresses for automatic router discovery and to communicate important routing information. For example, Open Shortest Path First (OSPF) uses the IP addresses 224.0.0.5 and 224.0.0.6 to exchange link-state information.

IANA assigns single multicast address requests for network protocols or network applications out of the 224.0.1.xxx address range. Multicast routers forward these multicast addresses.

### Globally Scoped Addresses

Addresses in the range 224.0.1.0 to 238.255.255.255 are called globally scoped addresses. These addresses are used to send multicast data between organizations across the Internet. Some of these addresses have been reserved by IANA for use by multicast applications. For example, the IP address 224.0.1.1 is reserved for Network Time Protocol (NTP).

### Source Specific Multicast Addresses

Addresses in the range 232.0.0.0/8 are reserved for Source Specific Multicast (SSM) by IANA. In Cisco IOS software, you can use the **ip pim ssm** command to configure SSM for arbitrary IP multicast addresses also. SSM is an extension of Protocol Independent Multicast (PIM) that allows for an efficient data delivery mechanism in one-to-many communications. SSM is described in the [“IP Multicast Delivery Modes”](#) section on page 1-22.

### GLOP Addresses

GLOP addressing (as proposed by RFC 2770, *GLOP Addressing in 233/8*) proposes that the 233.0.0.0/8 range be reserved for statically defined addresses by organizations that already have an AS number reserved. This practice is called GLOP addressing. The AS number of the domain is embedded into the second and third octets of the 233.0.0.0/8 address range. For example, AS 62010 is written in hexadecimal format as F23A. Separating the two octets F2 and 3A results in 242 and 58 in decimal format. These values result in a subnet of 233.242.58.0/24 that would be globally reserved for AS 62010 to use.

### Limited Scope Addresses

The range 239.0.0.0 to 239.255.255.255 is reserved as administratively or limited scoped addresses for use in private multicast domains. These addresses are constrained to a local group or organization. Companies, universities, and other organizations can use limited scope addresses to have local multicast applications that will not be forwarded outside their domain. Routers typically are configured with filters to prevent multicast traffic in this address range from flowing outside an autonomous system (AS) or any user-defined domain. Within an AS or domain, the limited scope address range can be further subdivided so that local multicast boundaries can be defined.

**Note**

Network administrators may use multicast addresses in this range, inside a domain, without conflicting with others elsewhere in the Internet.

## Layer 2 Multicast Addresses

Historically, network interface cards (NICs) on a LAN segment could receive only packets destined for their burned-in MAC address or the broadcast MAC address. In IP multicast, several hosts need to be able to receive a single data stream with a common destination MAC address. Some means had to be devised so that multiple hosts could receive the same packet and still be able to differentiate between several multicast groups. One method to accomplish this is to map IP multicast Class D addresses directly to a MAC address. Using this method, NICs can receive packets destined to many different MAC address.

Cisco Group Management Protocol (CGMP) is used on routers connected to Catalyst switches to perform tasks similar to those performed by IGMP. CGMP is necessary for those Catalyst switches that cannot distinguish between IP multicast data packets and IGMP report messages, both of which are addressed to the same group address at the MAC level.

## IP Multicast Delivery Modes

IP multicast delivery modes differ only for the receiver hosts, not for the source hosts. A source host sends IP multicast packets with its own IP address as the IP source address of the packet and a group address as the IP destination address of the packet.

### Any Source Multicast

For the Any Source Multicast (ASM) delivery mode, an IP multicast receiver host can use any version of IGMP to join a multicast group. This group is notated as G in the routing table state notation. By joining this group, the receiver host is indicating that it wants to receive IP multicast traffic sent by any source to group G. The network will deliver IP multicast packets from any source host with the destination address G to all receiver hosts in the network that have joined group G.

ASM requires group address allocation within the network. At any given time, an ASM group should only be used by a single application. When two applications use the same ASM group simultaneously, receiver hosts of both applications will receive traffic from both application sources. This may result in unexpected excess traffic in the network. This situation may cause congestion of network links and malfunction of the application receiver hosts.

**Note**

Release 12.2(33)MRB does not support Any Source Multicast.

## Source Specific Multicast

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core network technology for the Cisco implementation of IP multicast targeted for audio and video broadcast application environments and is described in RFC 3569. Source specific multicast consists of

- Protocol Independent Multicast source-specific mode (PIM-SSM)
- Internet Group Management Protocol Version 3 (IGMPv3)

For the SSM delivery mode, an IP multicast receiver host must use IGMP Version 3 (IGMPv3) to subscribe to channel (S,G). By subscribing to this channel, the receiver host is indicating that it wants to receive IP multicast traffic sent by source host S to group G. The network will deliver IP multicast packets from source host S to group G to all hosts in the network that have subscribed to the channel (S, G).

SSM does not require group address allocation within the network, only within each source host. Different applications running on the same source host must use different SSM groups. Different applications running on different source hosts can arbitrarily reuse SSM group addresses without causing any excess traffic on the network.

## Protocol Independent Multicast

The Protocol Independent Multicast (PIM) protocol maintains the current IP multicast service mode of receiver-initiated membership. PIM is not dependent on a specific unicast routing protocol; it is IP routing protocol independent and can leverage whichever unicast routing protocols are used to populate the unicast routing table, including Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and static routes. PIM uses unicast routing information to perform the multicast forwarding function.

Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the reverse path forwarding (RPF) check function instead of building up a completely independent multicast routing table. Unlike other routing protocols, PIM does not send and receive routing updates between routers.

PIM is defined in RFC 2362, [\*Protocol-Independent Multicast-Sparse Mode \(PIM-SM\): Protocol Specification\*](#).

## PIM Modes

Cisco IOS defines the following PIM modes:

- **PIM Dense Mode**—Uses a push model to flood multicast traffic to every corner of the network. This push model is a method for delivering data to the receivers without the receivers requesting the data. This method is efficient in certain deployments in which there are active receivers on every subnet in the network. Dense mode is not supported in Release 12.2(33)MRB.
- **PIM Sparse Mode**—Uses a pull model to deliver multicast traffic. Only network segments with active receivers that have explicitly requested the data will receive the traffic. PIM sparse mode is supported in Release 12.2(33)MRB.
- **Sparse-Dense Mode**—PIM runs sparse and dense mode according to the group mode; the interface is treated as dense mode if the group is in dense mode; the interface is treated in sparse mode if the group is in sparse mode. Sparse-dense mode is supported in Release 12.2(33)MRB.
- **Bidirectional PIM**—Traffic is routed only along a bidirectional shared tree that is rooted at the RP for the group. In bidir-PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. Bidirectional PIM is not supported in Release 12.2(33)MRB.

For more information about PIM modes, see the [Cisco IOS IP Multicast Configuration Guide, Release 12.2SR](#).

## Multicast Group Modes

In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. Cisco IOS supports four modes for a multicast group:

- **PIM Bidirectional mode**—Traffic is routed only along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group.
- **PIM Sparse mode**—Uses a unidirectional shared tree whose root node is called the rendezvous point (RP).
- **PIM Dense mode**—Dense mode operates using the broadcast (flood) and prune model.
- **PIM Source Specific Multicast (SSM) mode**—Datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined.

The MWR 2941 supports PIM Sparse mode and PIM SSM mode.

## Sparse Mode

Sparse mode operation centers around a single unidirectional shared tree whose root node is called the rendezvous point (RP). Sources must register with the RP to get their multicast traffic to flow down the shared tree by way of the RP. This registration process actually triggers a shortest path tree (SPT) Join by the RP toward the source when there are active receivers for the group in the network.

A sparse mode group uses the explicit join model of interaction. Receiver hosts join a group at a rendezvous point (RP). Different groups can have different RPs.

Multicast traffic packets flow down the shared tree to only those receivers that have explicitly asked to receive the traffic.



### Note

The Cisco MWR 2941 supports sparse mode with a single static Rendezvous Point.

For more information about sparse mode, see the [Cisco IOS IP Multicast Configuration Guide, Release 12.2SR](#).

## PIM Source Specific Multicast Mode

SSM is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for audio and video broadcast application environments and is described in RFC 3569. The following two Cisco IOS components together support the implementation of SSM:

- Protocol Independent Multicast source-specific mode (PIM-SSM)
- Internet Group Management Protocol Version 3 (IGMPv3)

Protocol Independent Multicast (PIM) SSM, or PIM-SSM, is the routing protocol that supports the implementation of SSM and is derived from PIM sparse mode (PIM-SM). IGMP is the Internet Engineering Task Force (IETF) standards track protocol used for hosts to signal multicast group membership to routers. IGMP Version 3 supports source filtering, which is required for SSM. For SSM to run with IGMPv3, SSM must be supported in the Cisco IOS router, the host where the application is running, and the application itself.

For more information about SSM, see the [Cisco IOS IP Multicast Configuration Guide, Release 12.2SR](#).

## Rendezvous Points

A rendezvous point (RP) is a role that a router performs when operating in PIM-SM mode. An RP is required only in networks running PIM-SM. In PIM-SM, only network segments with active receivers that have explicitly requested multicast data will be forwarded the traffic. This method of delivering multicast data is in contrast to the PIM dense mode (PIM-DM) model. In PIM-DM, multicast traffic is initially flooded to all segments of the network. Routers that have no downstream neighbors or directly connected receivers prune back the unwanted traffic.

An RP acts as the meeting place for sources and receivers of multicast data. In a PIM-SM network, sources must send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree. By default, when the first hop router of the receiver learns about the source, it will send a Join message directly to the source, creating a source-based distribution tree from the source to the receiver. This source tree does not include the RP unless the RP is located within the shortest path between the source and receiver.

In most cases, the placement of the RP in the network is not a complex decision. By default, the RP is needed only to start new sessions with sources and receivers. Consequently, the RP experiences little overhead from traffic flow or processing. In PIM version 2, the RP performs less processing than in PIM version 1 because sources must only periodically register with the RP to create state.

## Auto-RP

In the first version of PIM-SM, all leaf routers (routers directly connected to sources or receivers) were required to be manually configured with the IP address of the RP. This type of configuration is also known as static RP configuration. Configuring static RPs is relatively easy in a small network, but it can be laborious in a large, complex network.

Following the introduction of PIM-SM version 1, Cisco implemented a version of PIM-SM with the Auto-RP feature. Auto-RP automates the distribution of group-to-RP mappings in a PIM network. Auto-RP has the following benefits:

- Configuring the use of multiple RPs within a network to serve different groups is easy.

- Auto-RP allows load splitting among different RPs and arrangement of RPs according to the location of group participants.
- Auto-RP avoids inconsistent, manual RP configurations that can cause connectivity problems.

Multiple RPs can be used to serve different group ranges or serve as backups to each other. For Auto-RP to work, a router must be designated as an RP-mapping agent, which receives the RP-announcement messages from the RPs and arbitrates conflicts. The RP-mapping agent then sends the consistent group-to-RP mappings to all other routers. Thus, all routers automatically discover which RP to use for the groups they support.

**Note**

If you configure PIM in sparse mode or sparse-dense mode and do not configure Auto-RP, you must statically configure an RP.

**Note**

If router interfaces are configured in sparse mode, Auto-RP can still be used if all routers are configured with a static RP address for the Auto-RP groups.

To make Auto-RP work, a router must be designated as an RP mapping agent, which receives the RP announcement messages from the RPs and arbitrates conflicts. The RP mapping agent then sends the consistent group-to-RP mappings to all other routers by dense mode flooding. Thus, all routers automatically discover which RP to use for the groups they support. The Internet Assigned Numbers Authority (IANA) has assigned two group addresses, 224.0.1.39 and 224.0.1.40, for Auto-RP. One advantage of Auto-RP is that any change to the RP designation must be configured only on the routers that are RPs and not on the leaf routers. Another advantage of Auto-RP is that it offers the ability to scope the RP address within a domain. Scoping can be achieved by defining the time-to-live (TTL) value allowed for the Auto-RP advertisements.

Each method for configuring an RP has its own strengths, weaknesses, and level of complexity. In conventional IP multicast network scenarios, we recommend using Auto-RP to configure RPs because it is easy to configure, well-tested, and stable. The alternative ways to configure an RP are static RP, Auto-RP, and bootstrap router.

## Bootstrap Router

Another RP selection model called bootstrap router (BSR) was introduced after Auto-RP in PIM-SM version 2. BSR performs similarly to Auto-RP in that it uses candidate routers for the RP function and for relaying the RP information for a group. RP information is distributed through BSR messages, which are carried within PIM messages. PIM messages are link-local multicast messages that travel from PIM router to PIM router. Because of this single hop method of disseminating RP information, TTL scoping cannot be used with BSR. A BSR performs similarly as an RP, except that it does not run the risk of reverting to dense mode operation, and it does not offer the ability to scope within a domain.

## Multicast Source Discovery Protocol

In the PIM sparse mode model, multicast sources and receivers must register with their local rendezvous point (RP). Actually, the router closest to a source or a receiver registers with the RP, but the key point to note is that the RP “knows” about all the sources and receivers for any particular group. RPs in other domains have no way of knowing about sources that are located in other domains. Multicast Source Discovery Protocol (MSDP) is an elegant way to solve this problem.

MSDP is a mechanism that allows RPs to share information about active sources. RPs know about the receivers in their local domain. When RPs in remote domains hear about the active sources, they can pass on that information to their local receivers. Multicast data can then be forwarded between the

domains. A useful feature of MSDP is that it allows each domain to maintain an independent RP that does not rely on other domains, but it does enable RPs to forward traffic between domains. PIM-SM is used to forward the traffic between the multicast domains.

The RP in each domain establishes an MSDP peering session using a TCP connection with the RPs in other domains or with border routers leading to the other domains. When the RP learns about a new multicast source within its own domain (through the normal PIM register mechanism), the RP encapsulates the first data packet in a Source-Active (SA) message and sends the SA to all MSDP peers. Each receiving peer uses a modified Reverse Path Forwarding (RPF) check to forward the SA, until the SA reaches every MSDP router in the interconnected networks—theoretically the entire multicast internet. If the receiving MSDP peer is an RP, and the RP has a (\*, G) entry for the group in the SA (there is an interested receiver), the RP creates (S,G) state for the source and joins to the shortest path tree for the source. The encapsulated data is decapsulated and forwarded down the shared tree of that RP. When the last hop router (the router closest to the receiver) receives the multicast packet, it may join the shortest path tree to the source. The MSDP speaker periodically sends SAs that include all sources within the domain of the RP.

MSDP was developed for peering between Internet service providers (ISPs). ISPs did not want to rely on an RP maintained by a competing ISP to provide service to their customers. MSDP allows each ISP to have its own local RP and still forward and receive multicast traffic to the Internet.

## Anycast RP

Anycast RP is a useful application of MSDP. Originally developed for interdomain multicast applications, MSDP used for Anycast RP is an intradomain feature that provides redundancy and load-sharing capabilities. Enterprise customers typically use Anycast RP for configuring a Protocol Independent Multicast sparse mode (PIM-SM) network to meet fault tolerance requirements within a single multicast domain.

In Anycast RP, two or more RPs are configured with the same IP address on loopback interfaces. The Anycast RP loopback address should be configured with a 32-bit mask, making it a host address. All the downstream routers should be configured to “know” that the Anycast RP loopback address is the IP address of their local RP. IP routing automatically will select the topologically closest RP for each source and receiver. Assuming that the sources are evenly spaced around the network, an equal number of sources will register with each RP. That is, the process of registering the sources will be shared equally by all the RPs in the network.

Because a source may register with one RP and receivers may join to a different RP, a method is needed for the RPs to exchange information about active sources. This information exchange is done with MSDP.

In Anycast RP, all the RPs are configured to be MSDP peers of each other. When a source registers with one RP, an SA message will be sent to the other RPs informing them that there is an active source for a particular multicast group. The result is that each RP will know about the active sources in the area of the other RPs. If any of the RPs were to fail, IP routing would converge and one of the RPs would become the active RP in more than one area. New sources would register with the backup RP. Receivers would join toward the new RP and connectivity would be maintained.



### Note

The RP is normally needed only to start new sessions with sources and receivers. The RP facilitates the shared tree so that sources and receivers can directly establish a multicast data flow. If a multicast data flow is already directly established between a source and the receiver, then an RP failure will not affect that session. Anycast RP ensures that new sessions with sources and receivers can begin at any time.

## Multicast Forwarding

Forwarding of multicast traffic is accomplished by multicast-capable routers. These routers create distribution trees that control the path that IP multicast traffic takes through the network in order to deliver traffic to all receivers.

Multicast traffic flows from the source to the multicast group over a distribution tree that connects all of the sources to all of the receivers in the group. This tree may be shared by all sources (a shared tree) or a separate distribution tree can be built for each source (a source tree). The shared tree may be one-way or bidirectional.

Before describing the structure of source and shared trees, it is helpful to explain the notations that are used in multicast routing tables. These notations include the following:

- (S,G) = (unicast source for the multicast group G, multicast group G)
- (\*,G) = (any source for the multicast group G, multicast group G)

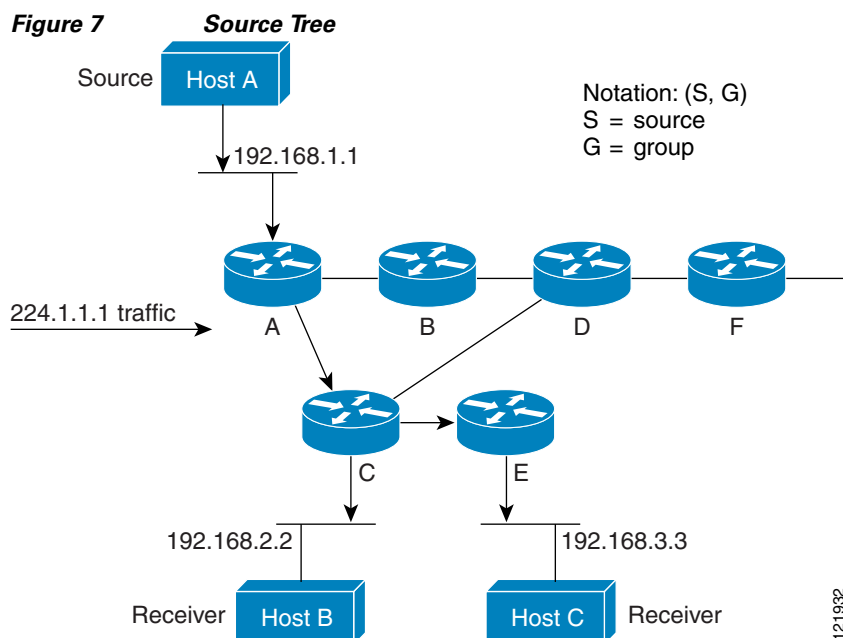
The notation of (S,G), pronounced “S comma G,” enumerates a shortest path tree where S is the IP address of the source and G is the multicast group address.

Shared trees are (\*,G) and the source trees are (S,G) and always rooted at the sources.

### Multicast Distribution Source Tree (Shortest Path Tree)

The simplest form of a multicast distribution tree is a source tree. A source tree has its root at the source host and has branches forming a spanning tree through the network to the receivers. Because this tree uses the shortest path through the network, it is also referred to as a shortest path tree (SPT).

Figure 7 shows an example of an SPT for group 224.1.1.1 rooted at the source, Host A, and connecting two receivers, Hosts B and C.



Using standard notation, the SPT for the example shown in Figure 7 would be (192.168.1.1, 224.1.1.1).

The (S,G) notation implies that a separate SPT exists for each individual source sending to each group—which is correct.

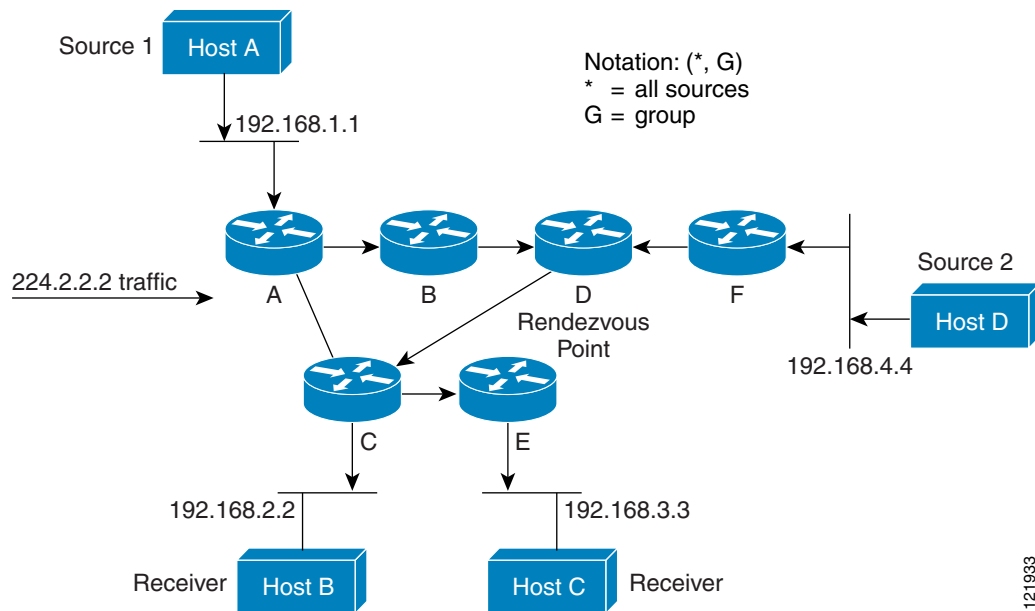


## Multicast Distribution Shared Tree

Unlike source trees that have their root at the source, shared trees use a single common root placed at some chosen point in the network. This shared root is called a rendezvous point (RP).

Figure 8 shows a shared tree for the group 224.2.2.2 with the root located at Router D. This shared tree is unidirectional. Source traffic is sent towards the RP on a source tree. The traffic is then forwarded down the shared tree from the RP to reach all of the receivers (unless the receiver is located between the source and the RP, in which case it will be serviced directly).

**Figure 8 Shared Distribution Tree**



In this example, multicast traffic from the sources, Hosts A and D, travels to the root (Router D) and then down the shared tree to the two receivers, Hosts B and C. Because all sources in the multicast group use a common shared tree, a wildcard notation written as (\*, G), pronounced “star comma G,” represents the tree. In this case, \* means all sources, and G represents the multicast group. Therefore, the shared tree shown in Figure 8 would be written as (\*, 224.2.2.2).

Both source trees and shared trees are loop-free. Messages are replicated only where the tree branches. Members of multicast groups can join or leave at any time; therefore the distribution trees must be dynamically updated. When all the active receivers on a particular branch stop requesting the traffic for a particular multicast group, the routers prune that branch from the distribution tree and stop forwarding traffic down that branch. If one receiver on that branch becomes active and requests the multicast traffic, the router will dynamically modify the distribution tree and start forwarding traffic again.

## Source Tree Advantage

Source trees have the advantage of creating the optimal path between the source and the receivers. This advantage guarantees the minimum amount of network latency for forwarding multicast traffic. However, this optimization comes at a cost. The routers must maintain path information for each source. In a network that has thousands of sources and thousands of groups, this overhead can quickly become a resource issue on the routers. Memory consumption from the size of the multicast routing table is a factor that network designers must take into consideration.

## Shared Tree Advantage

Shared trees have the advantage of requiring the minimum amount of state in each router. This advantage lowers the overall memory requirements for a network that only allows shared trees. The disadvantage of shared trees is that under certain circumstances the paths between the source and receivers might not be the optimal paths, which might introduce some latency in packet delivery. For example, in [Figure 8](#) the shortest path between Host A (source 1) and Host B (a receiver) would be Router A and Router C. Because we are using Router D as the root for a shared tree, the traffic must traverse Routers A, B, D and then C. Network designers must carefully consider the placement of the rendezvous point (RP) when implementing a shared tree-only environment.

In unicast routing, traffic is routed through the network along a single path from the source to the destination host. A unicast router does not consider the source address; it considers only the destination address and how to forward the traffic toward that destination. The router scans through its routing table for the destination address and then forwards a single copy of the unicast packet out the correct interface in the direction of the destination.

In multicast forwarding, the source is sending traffic to an arbitrary group of hosts that are represented by a multicast group address. The multicast router must determine which direction is the upstream direction (toward the source) and which one is the downstream direction (or directions) toward the receivers. If there are multiple downstream paths, the router replicates the packet and forwards it down the appropriate downstream paths (best unicast route metric)—which is not necessarily all paths. Forwarding multicast traffic away from the source, rather than to the receiver, is called Reverse Path Forwarding (RPF). RPF is described in the following section.

## Reverse Path Forwarding (RPF)

In unicast routing, traffic is routed through the network along a single path from the source to the destination host. A unicast router does not consider the source address; it considers only the destination address and how to forward the traffic toward that destination. The router scans through its routing table for the destination network and then forwards a single copy of the unicast packet out the correct interface in the direction of the destination.

In multicast forwarding, the source is sending traffic to an arbitrary group of hosts that are represented by a multicast group address. The multicast router must determine which direction is the upstream direction (toward the source) and which one is the downstream direction (or directions) toward the receivers. If there are multiple downstream paths, the router replicates the packet and forwards it down the appropriate downstream paths (best unicast route metric)—which is not necessarily all paths. Forwarding multicast traffic away from the source, rather than to the receiver, is called Reverse Path Forwarding (RPF). RPF is an algorithm used for forwarding multicast datagrams.

Protocol Independent Multicast (PIM) uses the unicast routing information to create a distribution tree along the reverse path from the receivers towards the source. The multicast routers then forward packets along the distribution tree from the source to the receivers. RPF is a key concept in multicast forwarding. It enables routers to correctly forward multicast traffic down the distribution tree. RPF makes use of the existing unicast routing table to determine the upstream and downstream neighbors. A router will forward a multicast packet only if it is received on the upstream interface. This RPF check helps to guarantee that the distribution tree will be loop-free.

## RPF Check

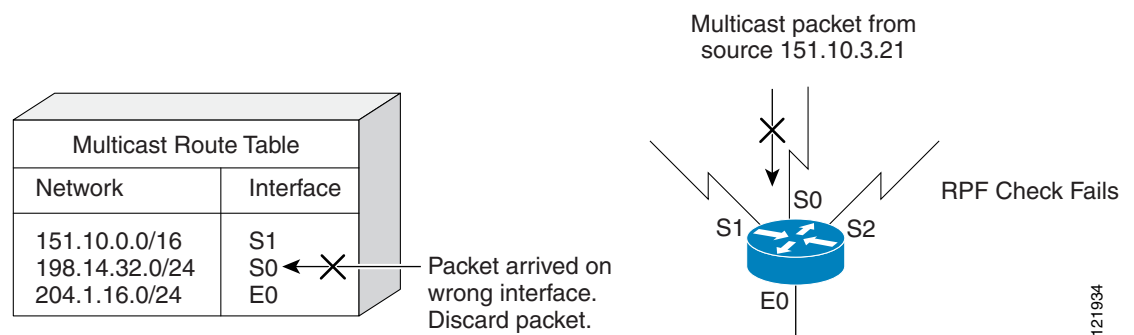
When a multicast packet arrives at a router, the router performs an RPF check on the packet. If the RPF check succeeds, the packet is forwarded. Otherwise, it is dropped.

For traffic flowing down a source tree, the RPF check procedure works as follows:

1. The router looks up the source address in the unicast routing table to determine if the packet has arrived on the interface that is on the reverse path back to the source.
2. If the packet has arrived on the interface leading back to the source, the RPF check succeeds and the packet is forwarded out the interfaces present in the outgoing interface list of a multicast routing table entry.
3. If the RPF check in Step 2 fails, the packet is dropped.

Figure 9 shows an example of an unsuccessful RPF check.

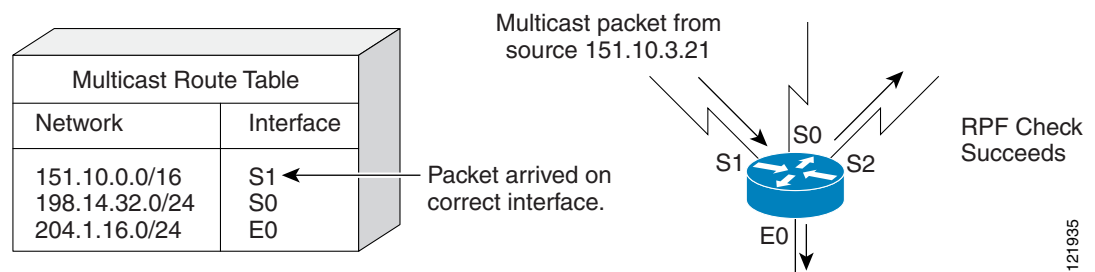
**Figure 9 RPF Check Fails**



As Figure 9 illustrates, a multicast packet from source 151.10.3.21 is received on serial interface 0 (S0). A check of the unicast route table shows that S1 is the interface this router would use to forward unicast data to 151.10.3.21. Because the packet has arrived on interface S0, the packet is discarded.

Figure 10 shows an example of a successful RPF check.

**Figure 10 RPF Check Succeeds**



In this example, the multicast packet has arrived on interface S1. The router refers to the unicast routing table and finds that S1 is the correct interface. The RPF check passes, and the packet is forwarded.

For more information about multicast routing, see the [Cisco IOS IP Multicast Configuration Guide, Release 12.2SR](#). For instructions on how to configure multicast routing, see the “Configuring IP Multicast” section on page 4-64.

## MLPPP Optimization Features

The Cisco MWR 2941 supports several features that improve the performance of Multilink Point-to-Point Protocol (MLPPP) connections and related applications such as PWE3 over MLPPP and IP over MLPPP.

### Distributed Multilink Point-to-Point Protocol (dMLPPP) Offload

Distributed Multilink Point-to-Point Protocol (dMLPPP) allows you to combine T1 or E1 connections into a bundle that has the combined bandwidth of all of the connections in the bundle, providing improved capacity and CPU utilization over MLPPP. The dMLPPP offload feature improves the performance for traffic in dMLPPP applications such as PWE3 over MLPPP and IP over MLPPP by shifting processing of this traffic from the main CPU to the network processor.

The Cisco MWR 2941 supports up to four serial links per T1/E1 connection and up to 24 MLPPP bundles. You can use the fixed T1/E1 ports to create up to 64 MLPPP links; if you install two four-port T1/E1 HWICs, you can create up to 96 MLPPP links.

The MWR 2941 implementation of multilink (dMLPPP) uses interleaving to allow short, delay-sensitive packets to be transmitted within a predictable amount of time. Interleaving allows the MWR 2941 to interrupt the transmission of delay-insensitive packets in order to transmit delay-sensitive packets. You can also adjust the responsiveness of the MWR 2941 to delay-sensitive traffic by adjusting the maximum fragment size; this value determines the maximum delay that a delay-sensitive packet can encounter while the MWR 2941 transmits queued fragments of delay-insensitive traffic.

### Multiclass MLPPP

The MWR 2941 implementation of dMLPPP also supports Multiclass MLPPP. Multiclass MLPPP is an extension to MLPPP functionality that allows you to divide traffic passing over a multilink bundle into several independently sequenced streams or classes. Each multiclass MLPPP class has a unique sequence number, and the receiving network peer processes each stream independently. The multiclass MLPPP standard is defined in RFC 2686.

The MWR 2941 supports the following multiclass MLPPP classes:

- Class 0—Data traffic that is subject to normal MLPPP fragmentation. Appropriate for non-delay-sensitive traffic.
- Class 1—Data traffic that can be interleaved but not fragmented. Appropriate for delay-sensitive traffic such as voice.

For instructions on how to configure MLPPP backhaul, see the [“Configuring MLPPP Backhaul” section on page 4-49](#).



#### Note

The Cisco MWR 2941 does not support some PPP and MLPPP options when the bundle is offloaded to the network processor; you can retain these options by disabling MLPPP and IPHC offloading for a given bundle. For more information, see the [“MLPPP Offload” section on page 4-58](#).



#### Note

The output for the **show ppp multilink** command for an offloaded MLPPP bundle differs from the output for a non-offloaded bundle. For more information, see [Appendix B, “Cisco MWR 2941 Router Command Reference.”](#)

## Layer 3 Virtual Private Networks

A Virtual Private Network (VPN) is an IP-based network that delivers private network services over a public infrastructure. VPNs allow you to create a set of sites that can communicate privately over the Internet or other public or private networks.

A conventional VPN consists of a full mesh of tunnels or permanent virtual circuits (PVCs) connecting all of the sites within the VPN. This type of VPN requires changes to each edge device in the VPN in order to add a new site. Layer 3 VPNs are easier to manage and expand than conventional VPNs because they use layer 3 communication protocols and are based on a peer model. The peer model enables the service provider and customer to exchange Layer 3 routing information, enabling service providers to relay data between customer sites without customer involvement. The peer model also provides improved security of data transmission between VPN sites because data is isolated between improves security between VPN sites.

The Cisco MWR 2941 supports the following MPLS VPN types:

- **Basic Layer 3 VPN**—Provides a VPN private tunnel connection between customer edge (CE) devices in the service provider network. The provider edge (PE) router uses Multiprotocol Border Gateway Protocol (MP-BGP) to distribute VPN routes and MPLS Label Distribution Protocol (LDP) to distribute Interior Gateway Protocol (IGP) labels to the next-hop PE router.
- **MPLS Carrier Supporting Carrier (CSC) VPN**—Enables an MPLS VPN-based service provider to allow other service providers to use a segment of its backbone network. MPLS CSC VPNs use MPLS LDP to distribute MPLS labels and IGP to distribute routes.
- **Inter-Autonomous System (AS) VPN**—An inter-AS VPN allows service providers running separate networks to jointly offer MPLS VPN services to the same end customer; an inter-AS VPN can begin at one customer site and traverse multiple service provider backbones before arriving at another customer site.

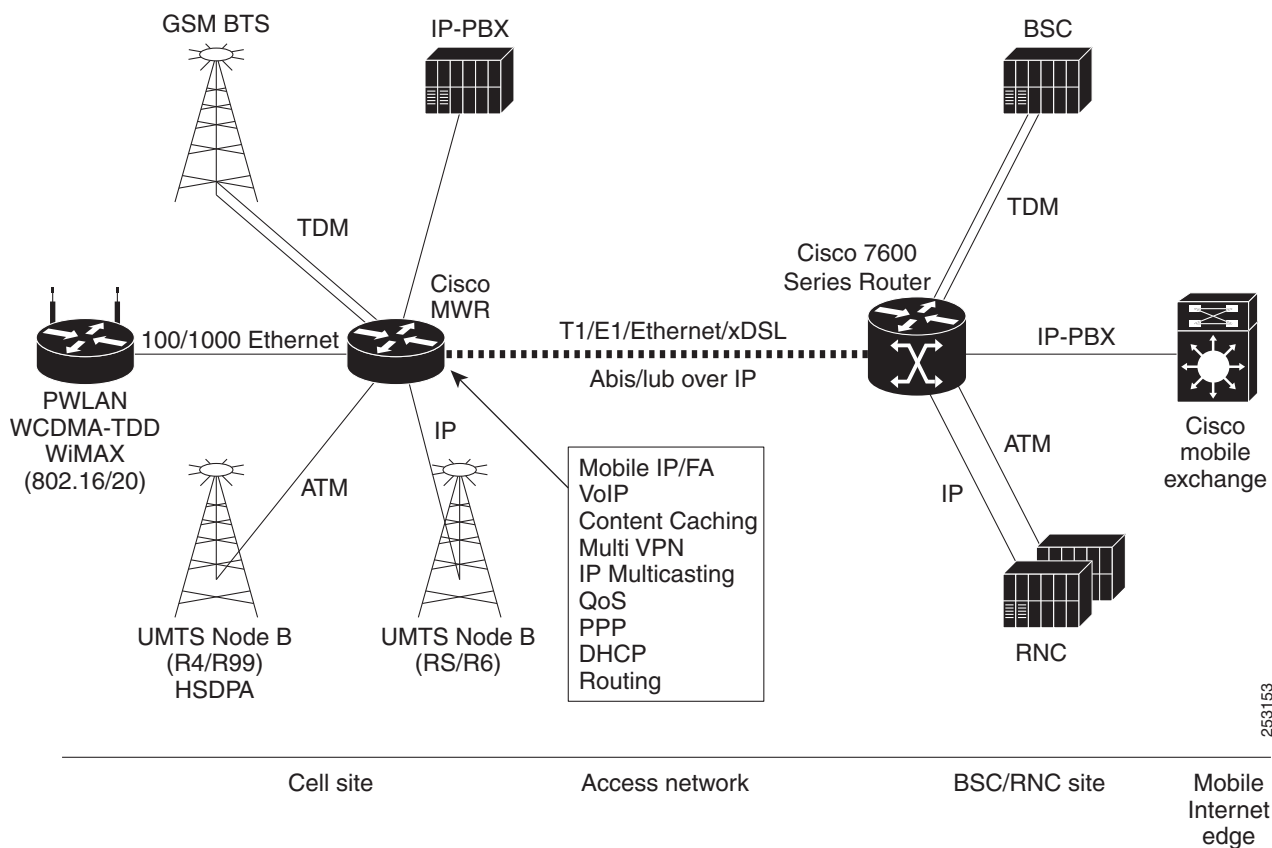
For instructions on how to configure an layer 3 VPN, see the [“Layer 3 Virtual Private Networks” section on page 1-33](#).

## Intelligent Cell Site IP Services

The Cisco RAN-O and IP-RAN solutions allow you to deliver profit-enhancing services. This is achieved through the set of IP networking features supported in Cisco IOS software that extends to the cell site (see [Figure 1-11 on page 1-34](#)).

### Cell Site Points-of-Presence

The cell site becomes a physical Point-of-Presence (POP) from which to offer hotspot services, or voice and wired ISP services, to nearby enterprises and residences. Because many cell sites are located in and around downtown areas, hotels, airports, and convention centers, they make attractive sites for co-locating public wireless LAN (PWLAN) access points and other wireless data overlays. Many of these wireless data radios are IP-based. IP networking features, like Mobile IP, VoIP, IP Multicast, VPN, and content caching, enable delivery of new revenue-generating services over these radios. The corresponding traffic “rides for free” on the spare backhaul bandwidth made available by Cisco Abis solutions (see [Figure 1-11](#)).

**Figure 1-11 Cisco MWR 2941 Router in a Cell Site POP—Example**

## Quality of Service

This section describes the Quality of Service (QoS) features on the Cisco MWR 2941. The Cisco MWR 2941 supports the following QoS features:

- [Traffic Classification](#)
- [Traffic Marking](#)
- [Traffic Queuing](#)
- [Traffic Shaping](#)



### Note

The Cisco MWR 2941 support for QoS varies based on the interface and traffic type. For more information about the QoS limitations, see the [“Configuring Quality of Service \(QoS\)”](#) section on page 4-88.

For instructions on how to configure QoS on the Cisco MWR 2941, see the [“Configuring Quality of Service \(QoS\)”](#) section on page 4-88.

## Traffic Classification

Classifying network traffic allows you to organize packets into traffic classes based on whether the traffic matches specific criteria. Classifying network traffic is the foundation for enabling many QoS features on your network. For instructions on how to configure traffic classification, see the [“Configuring Classification” section on page 4-95](#).

## Traffic Marking

Marking network traffic allows you to set or modify the attributes for packets in a defined traffic class. You can use marking with traffic classification to configure variety of QoS features for your network. For instructions on how to configure traffic marking, see the [“Configuring Marking” section on page 4-97](#).

## Traffic Queuing

The Cisco MWR 2941 supports class-based WFQ (CBWFQ) for congestion management. CBWFQ extends the standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria such as input interface. Packets satisfying the match criteria for a class constitute the traffic for that class. For more instructions on how to configure traffic queuing, see the [“Configuring Congestion Management” section on page 4-101](#).

## Traffic Shaping

Regulating the packet flow on the network is also known as traffic shaping. Traffic shaping allows you to control the speed of traffic leaving an interface. This way, you can match the flow of the traffic to the speed of the interface receiving the packet.

The Cisco MWR 2941 supports Class-Based Traffic Shaping. Class-Based Traffic Shaping allows you to regulate the flow of packets leaving an interface on a per-traffic-class basis, matching the packet flow to the speed of the interface. For more instructions on how to configure traffic shaping, see the [“Configuring Shaping” section on page 4-103](#).

# Network Management Features

This section provides an overview of the network management features for the Cisco MWR 2941. For more information about management features on the Cisco MWR 2941, see the [“Monitoring and Managing the Cisco MWR 2941 Router” section on page 4-107](#).

## Cisco Mobile Wireless Transport Manager (MWTM)

You can use Cisco Mobile Wireless Transport Manager (MWTM), to monitor and manage the Cisco MWR 2941. Cisco MWTM addresses the element-management requirements of mobile operators and provides fault, configuration, and troubleshooting capability. For more information about MWTM, see [http://www.cisco.com/en/US/products/ps6472/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6472/tsd_products_support_series_home.html).

## Cisco Active Network Abstraction (ANA)

You can also use Cisco Active Network Abstraction (ANA) to manage the Cisco MWR 2941. Cisco ANA is a powerful, next-generation network resource management solution designed with a fully distributed OSS mediation platform which abstracts the network, its topology and its capabilities from the physical elements. Its virtual nature provides customers with a strong and reliable platform for service activation, service assurance and network management. For more information about ANA, see [http://www.cisco.com/en/US/products/ps6776/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6776/tsd_products_support_series_home.html).

## SNMP MIB Support

To view the current MIBs that the Cisco MWR 2941 supports, see the *Release Notes for Cisco MWR 2941-DC Mobile Wireless Edge Router for Cisco IOS Release 12.4(20)MR*.

For instructions on how to configure MIBs on the Cisco MWR 2941, see the “Configuring SNMP Support” section on page 4-108 and the “Enabling Remote Network Management” section on page 4-112.

## Cisco Networking Services (CNS)

Cisco Networking Services (CNS) is a collection of services that can provide remote configuration of Cisco IOS networking devices and remote execution of some command-line interface (CLI) commands. CNS allows a Cisco MWR 2941 deployed and powered on in the field to automatically download its configuration.

**Note**

The Cisco MWR 2941 only supports CNS over motherboard Ethernet interfaces. Other interface types do not support CNS.

For instructions on how to configure CNS, see the “Configuring Cisco Networking Services (CNS)” section on page 4-115.

## Limitations and Restrictions

The following sections describe the limitations and restrictions that apply to the Cisco MWR 2941 router.

## Hardware Limitations and Restrictions

To view a list of supported hardware and restrictions for the Cisco MWR 2941, see the *Release Notes for Cisco MWR 2941-DC Mobile Wireless Edge Router for Cisco IOS Release 12.2(33)MRB*.

**Caution**

The Cisco MWR 2941 does not support online insertion and removal (OIR) of HWIC cards. Attempts to perform OIR on a card in a powered-on router might cause damage to the card.



## Software Limitations and Restrictions

For information about software limitations and restrictions for the Cisco MWR 2941, see the *Release Notes for Cisco MWR 2941-DC Mobile Wireless Edge Router for Cisco IOS Release 12.2(33)MRB*.





## CHAPTER 2

# Cisco IOS Software Basics

---

This chapter provides an overview of the Cisco IOS software. Read this section before you configure the router by using the command-line interface (CLI). This chapter includes the following topics:

- [Getting Help, page 2-1](#)
- [Understanding Command Modes, page 2-2](#)
- [Undoing a Command or Feature, page 2-3](#)
- [Saving Configuration Changes, page 2-3](#)

Understanding this information saves you time as you use the CLI. If you have never used the Cisco IOS software or if you need a review, read this chapter before you proceed. If you are already familiar with the Cisco IOS software, go to [Chapter 3, “First-Time Configuration.”](#)

## Getting Help

Use the question mark (?) and arrow keys to help you enter commands:

- For a list of available commands, enter a question mark:  
`Router> ?`
- To complete a command, enter a few known characters followed by a question mark (with no space):  
`Router> s?`
- For a list of command variables, enter the command followed by a space and a question mark:  
`Router> show ?`
- To redisplay a command that you previously entered, press the **Up Arrow** key. Continue to press the **Up Arrow** key to see more commands.

# Understanding Command Modes

The Cisco IOS user interface is used in various command modes. Each command mode permits you to configure different components on your router. The commands available at any given time depend on which command mode you are in. Entering a question mark (?) at a prompt displays a list of commands available for that command mode. The following table lists the most common command modes.

Command Mode	Access Method	Router Prompt Displayed	Exit Method
User EXEC	Log in.	Router>	Use the <b>logout</b> command.
Privileged EXEC	From user EXEC mode, enter the <b>enable</b> command.	Router#	To exit to user EXEC mode, use the <b>disable</b> , <b>exit</b> , or <b>logout</b> command.
Global configuration	From the privileged EXEC mode, enter the <b>configure terminal</b> command.	Router (config)#	To exit to privileged EXEC mode, use the <b>exit</b> or <b>end</b> command, or press <b>Ctrl-Z</b> .
Interface configuration	From the global configuration mode, enter the <b>interface type number</b> command, such as <b>interface serial 0/0</b> .	Router (config-if)#	To exit to global configuration mode, use the <b>exit</b> command.  To exit directly to privileged EXEC mode, press <b>Ctrl-Z</b> .



## Timesaver

Each command mode restricts you to a subset of commands. If you have trouble entering a command, check the prompt and enter the question mark (?) to see a list of available commands. You might be in the incorrect command mode or be using an incorrect syntax.

In the following example, notice how the prompt changes after each command to indicate a new command mode:

```
Router> enable
Password: <enable password>
Router# configure terminal
Router (config)# interface serial 0/0
Router (config-if)# line 0
Router (config-line)# controller t1 0
Router (config-controller)# exit
Router (config)# exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

The last message is normal and does not indicate an error. Press **Return** to get the Router# prompt.



## Note

You can press **Ctrl-Z** in any mode to immediately return to enable mode (Router#), instead of entering **exit**, which returns you to the previous mode.

## Undoing a Command or Feature

If you want to undo a command that you entered or if you want to disable a feature, enter the **no** keyword before most commands; for example, **no ip routing**.

## Saving Configuration Changes

To save your configuration changes to NVRAM, so that the changes are not lost during a system reload or power outage, enter the **copy running-config startup-config** command. For example:

```
Router# copy running-config startup-config  
Building configuration...
```

It might take a few minutes to save the configuration to NVRAM. After the configuration has been saved, the following message appears:

```
[OK]  
Router#
```





# CHAPTER 3

## First-Time Configuration

---

This chapter describes the actions to take before turning on your router for the first time. This chapter includes the following sections:

- [Understanding the Cisco MWR 2941 Router Interface Numbering, page 3-1](#)
- [Setup Command Facility, page 3-3](#)
- [Configuring Global Parameters, page 3-4](#)
- [Completing the Configuration, page 3-6](#)

## Understanding the Cisco MWR 2941 Router Interface Numbering

Each network interface on a Cisco MWR 2941 router is identified by a slot number and a port number.

[Figure 3-1](#) shows an example of interface numbering on a Cisco MWR 2941 router:

- Two HWIC ports (HWICs are ordered separately)
- Two built-in Gigabit Ethernet small form-factor pluggable (SFP) interfaces (labeled GE0 and GE1)
- Four built-in Gigabit Ethernet interfaces (labeled L2–L5)
- 16 E1/T1 ports (labeled C1AL–C15AL)



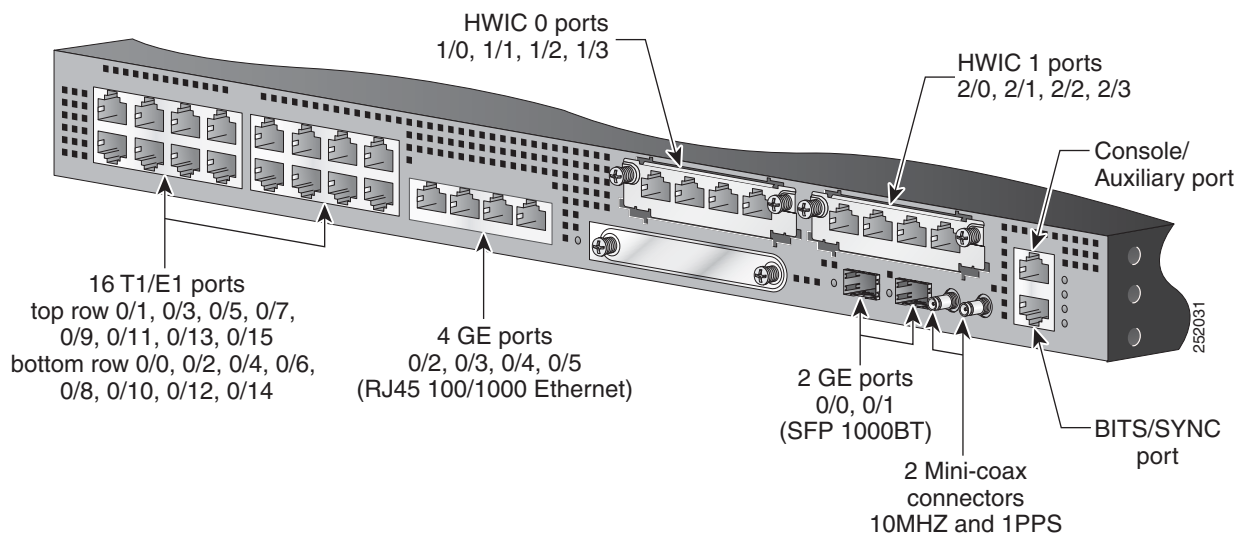
### Note

The two HWIC cards shown in [Figure 3-1](#) are not included with the Cisco MWR 2941 router; you must order them separately.



### Note

The Mini-coax timing connectors shown in [Figure 3-1](#) only apply to the Cisco MWR 2941-DC-A router; the Cisco MWR 2941-DC does not have these ports.

**Figure 3-1 Cisco MWR 2941 Router Port Numbers**

## Slot and Port Numbering

The Cisco MWR 2941 router chassis contains the following interface types:

- 16 T1/E1 ports, labeled “T1/E1”
- 4 RJ-45 jacks for copper Ethernet ports, labeled “100/1000” Ethernet
- 2 HWIC slots, labeled “HWIC0” and “HWIC1”
- 1 compact FLASH Type-II connector, labeled “Compact Flash”
- 2 SFP connectors for optical GE ports, labeled “GE0” and “GE1”
- 2 miniature coaxial connectors for 10MHZ and 1PPS timing



### Note

Miniature coaxial timing connectors are not included on all versions of the Cisco MWR 2941. You can verify your hardware version with the VID label on the back of the router; routers labeled with a VID of V01 or V02 do not include the timing connectors, while routers with VID V03 and higher include the connectors.

- 1 RJ-45 connector for Console/Auxiliary, labeled “CON/AUX”
- 1 RJ-45 jack for BITS interface, labeled “BITS”

The logical slot numbers are 0 for all built-in interfaces.

The numbering format is:

Interface type Slot number/Interface number

Interface (port) numbers begin at logical 0 for each interface type.



Following is an explanation of the slot/port numbering:

- Logical interface numbering for the built-in T1/E1 ports runs from 0/0 through 0/15. Interfaces are hardwired; therefore, port 0 is always logical interface 0/0, port 1 is always logical interface 0/1, and so on. Built-in T1/E1 ports are numbered bottom to top, left to right (bottom row numbered 0-2-4-6-8-10-12-14, top row numbered 1-3-5-7-9-11-13-15).
- When the 2 HWIC slots are used to expand the T1/E1 port density to 20 or 24 ports, logical interface numbering continues from 1/0 through 1/3 and 2/0 through 2/3. Logical interfaces for HWIC0 are always 1/0 through 1/3 and logical interfaces for HWIC1 are always 2/0 through 2/3. Because the interfaces are hardwired, HWIC0 port 0 is always logical interface 1/0, HWIC0 port 1 is always logical interface 1/1, HWIC1 port 0 is always logical interface 2/0, HWIC1 port 1 is always logical interface 2/1, and so on. Ports are numbered left to right for each HWIC.
- Logical interface numbering for the built-in Ethernet ports runs from 0/0 through 0/5. Because the interfaces are hard-wired, ports correspond to logical interface numbers. For example, port 0 is always logical interface 0/0, and port 1 is always logical interface 0/1. SFP ports are numbered left to right, 0 and 1; 100/1000 Ethernet ports are numbered left to right, 2 through 5.

## Setup Command Facility

The **setup** command facility prompts you for information that is required to start a router functioning quickly. The facility steps you through a basic configuration, including LAN interfaces.

If you prefer to configure the router manually or to configure a module or interface that is not included in the **setup** command facility, go to [Chapter 2, “Cisco IOS Software Basics.”](#) to familiarize yourself with the command-line interface (CLI). Then, go to [Chapter 4, “Configuring the Cisco MWR 2941 Router Using the CLI.”](#)



### Note

Cisco Networking Services (CNS) is a collection of services that can provide remote configuration of Cisco IOS networking devices and remote execution of some command-line interface (CLI) commands. CNS allows a Cisco MWR 2941 deployed and powered on in the field to automatically download its configuration. For more information about CNS, see the [“Cisco Networking Services \(CNS\)” section on page 1-36.](#)

## Before Starting Your Router

Before you power on your router and begin using the **setup** command facility, follow these steps:

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Set up the hardware and connect the console and network cables as described in the “Connecting Cables” section of the <i>Cisco MWR 2941-DC Router Hardware Installation Guide</i> . |
| <b>Step 2</b> | Configure your PC terminal emulation program for 9600 baud, 8 data bits, no parity, and 1 stop bit.   |
-

## Using the Setup Command Facility

The **setup** command facility appears in your PC terminal emulation program window. To create a basic configuration for your router, do the following:

- Complete the steps in the [Configuring Global Parameters, page 3-4](#).
- Complete the steps in the [Completing the Configuration, page 3-6](#).



### Note

If you make a mistake while using the setup command facility, you can exit the facility and run it again. Press **Ctrl-C**, and type **setup** at the enable mode prompt (1900#).

## Configuring Global Parameters

Use the following procedure to configure global parameters.

### Step 1

Power on the router. Messages appear in the terminal emulation program window.



### Caution

*Do not press any keys on the keyboard until the messages stop.* Any keys that you press during this time are interpreted as the first command entered after the messages stop, which might cause the router to power off and start over. Wait a few minutes. The messages stop automatically.

The messages look similar to the following:



### Note

The messages vary, depending on the Cisco IOS software image and interface modules in your router. This section is for reference only, and output might not match the messages on your console.

```
rommon 1 >boot
program load complete, entry point:0x80008000, size:0xc200

Initializing ATA monitor library.....
program load complete, entry point:0x80008000, size:0xc200

Initializing ATA monitor library.....
program load complete, entry point:0x80008000, size:0xc35eec
Self decompressing the image:
#####
#####
#####
#####
#####
#####
#####
#####
#####
#####
##### [OK]

Smart Init is enabled
smart init is sizing iomem
  ID  MEMORY_REQTYPE
0035C  0X005F3C00 MWR2941 Mainboard
        0X000F3BB0 public buffer pools
        0X00843000 public particle pools
```

TOTAL: 0X06894CB0

If any of the above Memory requirements are "UNKNOWN", you may be using an unsupported configuration or there is a software problem and system operation may be compromised.

Rounded IOMEM up to: 104Mb.

Using 20 percent iomem. [104Mb/512Mb]

#### Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, California 95134-1706

Cisco IOS Software, 2900 Software (MWR2900-IPRAN-M),  
Experimental Version 12.4(20050412:070057),  
Copyright (c) 1986-2009 by Cisco Systems, Inc.  
Compiled Sat 10-Jan-09 03:19 by cbrezove  
Image text-base:0x60008F60, data-base:0x6106A000

Cisco Systems, Inc. MWR-2941-DC (MPC8347E) processor (revision 0x400) with 41719  
6K/107092K bytes of memory.

Processor board ID

MPC8347E CPU Rev: Part Number 0x8032, Revision ID 0x300

1 RTM Module: ASM-M2900-TOP daughter card

6 Gigabit Ethernet interfaces

1 terminal line

128K bytes of non-volatile configuration memory.

125440K bytes of ATA CompactFlash (Read/Write)

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.

Use ctrl-c to abort configuration dialog at any prompt.

Default settings are in square brackets '[]'.

#### Step 2 To begin the initial configuration dialog, enter **yes** when the following message appears:

Basic management setup configures only enough connectivity  
for management of the system, extended setup will ask you  
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: **yes**

Configuring global parameters:

#### Step 3 Enter a hostname for the router (this example uses 2941-1).

Configuring global parameters:

Enter host name [Router]: **2941-1**

#### Step 4 Enter an enable secret password. This password is encrypted (more secure) and cannot be seen when viewing the configuration.

The enable secret is a password used to protect access to  
privileged EXEC and configuration modes. This password, after

entered, becomes encrypted in the configuration.  
 Enter enable secret: **ciscoenable**



**Note** When you enter the enable secret password, the password is visible while you type the it. After you enter the password, it becomes encrypted in the configuration.

- Step 5** Enter an enable password that is different from the enable secret password. This password is *not* encrypted (less secure) and can be seen when viewing the configuration.

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

Enter enable password: **ciscoenable**

- Step 6** To prevent unauthenticated access to the router through ports other than the console port, enter the virtual terminal password.

The virtual terminal password is used to protect access to the router over a network interface.

Enter virtual terminal password: **ciscoterminal**

- Step 7** Respond to the following prompts as appropriate for your network:

Configure SNMP Network Management? [yes]:  
 Community string [public]: **public**

- Step 8** The summary of interfaces appears. This list varies, depending on the network modules installed in your router.

Current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	NO	unset	up	up
GigabitEthernet0/1	unassigned	NO	unset	up	up

- Step 9** Specify the interface to be used to connect to the network management system.

Enter interface name used to connect to the management network from the above interface summary: **GigabitEthernet0/0**

- Step 10** Configure the specified interface as prompted.

Configuring interface GigabitEthernet0/0:  
 Configure IP on this interface? [no]:

## Completing the Configuration

When you have provided all of the information prompted for by the setup command facility, the configuration appears. Messages similar to the following appear:

The following configuration command script was created:

```
!
hostname 2941-1
enable secret 5 $1$5fH0$Z6Pr5Egtr5iNJ2nBg3i6y1 enable password ciscoenable line vty 0 4
```

```
password ciscoenablesnmp-server community public !
no ip routing

!
interface GigabitEthernet0/1
shutdown
!
end
```

To complete your router configuration, do the following:

---

**Step 1** A setup command facility prompt you to save this configuration.

[0] Go to the IOS command prompt without saving this config.  
[1] Return back to the setup without saving this config.  
[2] Save this configuration to nvram and exit.

Enter your selection [2]: **2**  
Building configuration...  
[OK]

Use the enabled mode 'configure' command to modify this configuration.

Press RETURN to get started!

If you answer:

- **no**—The configuration information that you entered is *not* saved, and you return to the router enable prompt. To return to the system configuration dialog, enter **setup**.
- **yes**—The configuration is saved, and you return to the EXEC prompt.

**Step 2** When the messages stop displaying in your window, press **Return** to view the command line prompt.

---

The 2941-1> prompt indicates that you are now at the CLI and you have just completed a basic router configuration. However, this is *not* a complete configuration. You must configure additional parameters by using the Cisco IOS software CLI as described in [Chapter 4, “Configuring the Cisco MWR 2941 Router Using the CLI.”](#)





## CHAPTER 4

# Configuring the Cisco MWR 2941 Router Using the CLI

---

This chapter describes how to use the Cisco IOS software command-line interface (CLI) to configure the Cisco MWR 2941 Mobile Wireless Edge Router and includes the following sections:

- [Verifying the Cisco IOS Software Version, page 4-1](#)
- [Configuration Sequence, page 4-1](#)
- [Monitoring and Managing the Cisco MWR 2941 Router, page 4-107](#)

For sample configurations, see [Appendix A, “Sample Configurations.”](#)

For additional configuration topics, see the Cisco IOS configuration guide and command reference publications. These publications are available online at [Cisco.com](http://Cisco.com), or as printed copies that you can order separately.



### Note

Be sure to review the [Chapter 2, “Cisco IOS Software Basics,”](#) before configuring your router; it contains important information that you need to successfully configure your router.

---

## Verifying the Cisco IOS Software Version

To implement the Cisco MWR 2941 router, Cisco IOS Release 12.4(19)MR2 or later must be installed on the router. To verify the version of Cisco IOS software, use the **show version** command.

The **show version** command displays the configuration of the system hardware, the software version, the names and sources of the configuration files, and the boot images.

## Configuration Sequence

The [“Summary of Steps” section on page 4-2](#) section provides the recommended primary configuration sequence for the Cisco MWR 2941 router. These steps have configuration substeps (or tasks) within the primary steps or tasks.



### Note

The installation of the Cisco MWR 2941 router and the Cisco T1/E1 interface card should be completed before attempting the configuration (see the [“Related Documentation” section on page xi](#) for more information).

---

The configuration sequence of the Cisco MWR 2941 router assumes that you will have already had some familiarity with the configuration of Cisco routers. It is also assumed that you are familiar with your own network configurations and that you are familiar with the Command Line Interface (CLI) used in configuring Cisco routers.

**Note**

For correct CLI syntax and format, see the [Appendix B, “Cisco MWR 2941 Router Command Reference”](#).

## Summary of Steps

To configure the Cisco MWR 2941 router, perform the following tasks.

1. [Configuring the Hostname and Password, page 4-2](#)
2. [Verifying the Hostname and Password, page 4-3](#)
3. [Configuring Gigabit Ethernet Interfaces, page 4-4](#)
4. [Configuring Layer 2 Interfaces, page 4-6](#)
5. [Configuring HWIC-9ESW Interfaces, page 4-11](#)
6. [Configuring VLANs, page 4-12](#)
7. [Configuring Resilient Ethernet Protocol \(REP\), page 4-15](#)
8. [Configuring Ethernet CFM, page 4-30](#)
9. [Configuring Ethernet Link Operations, Administration, and Maintenance \(OAM\), page 4-33](#)
10. [Configuring Ethernet Local Management Interface \(E-LMI\), page 4-38](#)
11. [Configuring Clocking and Timing, page 4-39](#)
12. [Configuring MLPPP Backhaul, page 4-49](#)
13. [Configuring Multiprotocol Label Switching \(MPLS\), page 4-58](#)
14. [Configuring Routing Protocols, page 4-59](#)
15. [Configuring BFD, page 4-59](#)
16. [Configuring IP Multicast, page 4-64](#)
17. [Configuring Pseudowire, page 4-73](#)
18. [Configuring Layer 3 Virtual Private Networks \(VPNs\), page 4-88](#)
19. [Configuring Quality of Service \(QoS\), page 4-88](#)
20. [Configuring Link Noise Monitor, page 4-104](#)
21. [Saving Configuration Changes, page 4-107](#)

## Configuring the Hostname and Password

Configure the hostname and set an encrypted password. Configuring a hostname allows you to distinguish between multiple Cisco routers. Setting an encrypted password allows you to prevent unauthorized configuration changes.



**Note**

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

To configure a hostname and to set an encrypted password, follow these steps:

**Step 1** Enter enable mode.

```
Router> enable
```

The Password prompt appears. Enter your password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

**Step 2** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

When the prompt changes to `Router(config)`, you have entered global configuration mode.

```
Router(config)#
```

**Step 3** Change the name of the router to a meaningful name. Substitute your hostname for `Router`.

```
Router(config)# hostname Router
```

```
Router(config)#
```

**Step 4** Enter an enable secret password. This password provides access to privileged EXEC mode. When you type **enable** at the EXEC prompt (`Router>`), you must enter the enable secret password to access configuration mode. Enter your secret password.

```
Router(config)# enable secret secret password
```

**Step 5** Exit back to global configuration mode.

```
Router(config)# exit
```

## Verifying the Hostname and Password

To verify that you have correctly configured the hostname and password, follow these steps:

**Step 1** Enter the **show config** command.

```
Router# show config
Using 1888 out of 126968 bytes
!
version XX.X
.
.
.
!
hostname Router
!
```

```
enable secret 5 $1$60L4$X2JY0woDc0.kqa1lo0/w8/  
.  
.  
.
```

**Step 2** Check the hostname and encrypted password, which appear near the top of the command output.

**Step 3** Exit global configuration mode and attempt to re-enter it using the new enable password:

```
Router# exit  
.  
.  
.  
Router con0 is now available  
Press RETURN to get started.  
Router> enable  
Password: password  
Router#
```

## Configuring Gigabit Ethernet Interfaces

To configure the Gigabit Ethernet (GE) interface on the Cisco MWR 2941, complete the following tasks:

- [Configuring the Interface Properties, page 4-4](#)
- [Setting the Speed and Duplex Mode, page 4-5](#)
- [Enabling the Interface, page 4-6](#)
- [Creating Backup Switch Interfaces, page 4-6](#)

## Configuring the Interface Properties

Perform a basic Gigabit Ethernet IP Address configuration by specifying the port adapter and aligning an IP address and subnet mask of the interface as follows.



### Note

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the Router# prompt.



### Note

The spanning tree-related commands described in this section are optional.

To configure the GE interface, follow these steps while in global configuration mode:

**Step 1** Specify the port adapter type and the location of the interface to be configured.

```
Router(config)# interface gigabitethernet slot/port  
Router(config-if)#
```

The *slot* is always 0 and the *port* is the number of the port (0 or 1).

**Step 2** To set the interface type, use the **switchport mode** command.

```
Router(config-if)# switchport mode {access | trunk}
```

- Step 3** To prioritize an interface when two bridges compete for position as the root bridge, use the **spanning tree port-priority** command.
- ```
Router(config-if)# spanning-tree port-priority port_priority
```
- Step 4** To calculate the path cost of STP on an interface, use the **spanning-tree cost** command.
- ```
Router(config-if)# spanning-tree cost port_cost
```
- Step 5** For interfaces that connect to end stations, you can use the **spanning-tree portfast** command to set the interface to move directly to the spanning-tree forwarding state when linkup occurs.
- ```
Router(config-if)# spanning-tree portfast
```
- Step 6** To enable Cisco Discovery Protocol (CDP) on the router, use the **cdp enable** command.
- ```
Router(config-if)# cdp enable
```
- 

## Setting the Speed and Duplex Mode

The Gigabit Ethernet ports of the Cisco MWR 2941 router can run in full or half-duplex mode—100 Mbps or 1000 Mbps (1 Gbps). The Cisco MWR 2941 router has an autonegotiation feature that allows the router to negotiate the speed and duplex mode with the corresponding interface at the other end of the connection.

Autonegotiation is the default setting for the speed and transmission mode.

When you configure an interface speed and duplex mode, follow these guidelines:

- If both ends of the line support autonegotiation, we highly recommend the use of default autonegotiation settings.
- When autonegotiation is turned on for either speed or duplex mode, it autonegotiates both speed and the duplex mode.
- If one interface supports autonegotiation, and the interface at the other end does not, configure the duplex mode and speed on both interfaces. If you use the autonegotiation setting on the supported side, the duplex mode setting is set at half-duplex.



**Note** In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the Router# prompt.

---

To configure speed and duplex operation, follow these steps while in interface configuration mode:

- Step 1** Specify the duplex operation.
- ```
Router(config-if)# duplex [auto | half | full]
```
- Step 2** Specify the speed.
- ```
Router(config-if)# speed [auto | 1000 | 100]
```
-

## Enabling the Interface

**Note**

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

After you configure the GE interface, enable it using the `no shutdown` command by following this step

```
Router(config-if)# no shutdown
```

## Creating Backup Switch Interfaces

You can use the following command to create a backup switch interface:

```
Router(config-if)# switchport backup interface interface_name preemption [forced |  
bandwidth | off] delay [time]
```

For more information about this command, see [switchport backup, page B-556](#)

For instructions on how to create VLANs on GE interfaces, see [Configuring VLANs, page 4-12](#).

## Configuring Layer 2 Interfaces

The Cisco MWR 2941 has an onboard layer 2 Gigabit Ethernet switch and supports HWICs with layer 2 interfaces. To configure the layer 2 interfaces on the Cisco MWR 2941, complete the following tasks:

- [Configuring a Range of Interfaces](#)
- [Defining a Range Macro](#)
- [Configuring Layer 2 Optional Interface Features](#)

### Configuring a Range of Interfaces

The `interface-range` command allows you to configure multiple interfaces at once. Follow these steps to configure an interface range.

**Step 1** Enter enable mode.

```
Router> enable  
Router#
```

**Step 2** Enter configuration mode.

```
Router# configure terminal  
Router(config)#
```

**Step 3** Use the `interface-range` command to select a range on interfaces to configure. You can specify a range that includes both VLANs and physical interfaces.

```
Router(config)# interface range GigabitEthernet 0/1 - 3
```

## Defining a Range Macro

A range macro allows you to create a name that defines a range on interfaces on the Cisco MWR 2941. Follow these steps to configure an interface range macro.

---

**Step 1** Enter enable mode.

```
Router> enable
Router#
```

**Step 2** Enter configuration mode.

```
Router# configure terminal
Router(config)#
```

**Step 3** Use the **interface-range** command to define the macro.

```
Router(config)# define interface-range first_three GigabitEthernet0/1 - 2
```

You can use the **show running-configuration** command to verify the interface-range macro configuration.

---

## Configuring Layer 2 Optional Interface Features

- [Interface Speed and Duplex Configuration Guidelines](#)
- [Configuring the Interface Speed](#)
- [Configuring the Interface Duplex Mode](#)
- [Configuring a Description for an Interface](#)
- [Configuring a Layer 2 Interface as a Layer 2 Trunk](#)
- [Configuring a Layer 2 Interface as Layer 2 Access](#)

### Interface Speed and Duplex Configuration Guidelines

When configuring an interface speed and duplex mode, note these guidelines:

- Speed and duplex commands only apply to FastEthernet interfaces. They do not apply to the onboard Gigabit Ethernet ports.
- If both ends of the line support autonegotiation, we highly recommend the default auto negotiation settings.
- If one interface supports auto negotiation and the other end does not, configure duplex and speed on both interfaces; do not use the auto setting on the supported side.
- Both ends of the line need to be configured to the same setting; for example, both hard-set or both auto-negotiate. Mismatched settings are not supported.



#### Caution

Changing the interface speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

---

## Configuring the Interface Speed

Follow these steps to configure the speed of a layer 2 interface.

- 
- Step 1** Enter enable mode.
- ```
Router> enable
Router#
```
- Step 2** Enter configuration mode.
- ```
Router# configure terminal
Router(config)#
```
- Step 3** Enter configuration for the interface that you want to modify.
- ```
Router(config)# interface fastethernet 1/0
```
- Step 4** Specify the interface speed. You can set an interface to 10 Mbps, 100 Mbps, or autonegotiate.
- ```
Router(config-if)# speed [10 | 100 | auto ]
```
- 

## Configuring the Interface Duplex Mode

Follow these steps below to set the duplex mode of a layer 2 interface.

- 
- Step 1** Enter enable mode.
- ```
Router> enable
Router#
```
- Step 2** Enter configuration mode.
- ```
Router# configure terminal
Router(config)#
```
- Step 3** Enter configuration for the interface that you want to modify.
- ```
Router(config)# interface fastethernet 1/1
```
- Step 4** Use the **duplex** command to set the interface to send traffic at full duplex, half duplex, or to autonegotiate its duplex setting.
- ```
Router(config-if)# duplex [auto | full | half]
```

You can use the **show interfaces** command to verify the duplex configuration.

**Note**

If you set the port speed to auto on a 10/100-Mbps Ethernet interface, the interface auto-negotiates the speed and duplex settings. You cannot change the duplex mode of interfaces set to auto-negotiation.

---

## Configuring a Description for an Interface

You can add a description of an interface to help you remember its function. The description appears in the output of the following commands: **show configuration**, **show running-config**, and **show interfaces**.

- 
- Step 1** Enter enable mode.
- ```
Router> enable
Router#
```
- Step 2** Enter configuration mode.
- ```
Router# configure terminal
Router(config)#
```
- Step 3** Enter configuration for the interface that you want to modify.
- ```
Router(config)# interface fastethernet 0/1
```
- Step 4** Use the **description** command to assign a description to the interface.
- ```
Router(config-if)# description newinterface
```
- 

## Configuring a Layer 2 Interface as a Layer 2 Trunk

Follow these steps to configure an interface as a Layer 2 trunk.

- 
- Step 1** Enter enable mode.
- ```
Router> enable
Router#
```
- Step 2** Enter configuration mode.
- ```
Router# configure terminal
Router(config)#
```
- Step 3** Enter configuration for the interface that you want to modify.
- ```
Router(config)# interface gigabitethernet 0/1
Router(config-if)#
```
- Step 4** Shut down the interface.
- ```
Router(config-if)# shutdown
```
- Step 5** Use the **switchport mode trunk** command to configure the interface as a Layer 2 trunk.
- ```
Router(config-if)# switchport mode trunk
```



**Note** The encapsulation is always set to dot1q.

- 
- Step 6** If you are configuring an 802.1Q trunk, specify the native VLAN. Otherwise, proceed to the next step.
- ```
Router(config-if)# switchport trunk native vlan 1
```
- Step 7** Use the **switchport trunk allowed vlan** command to configure the list of VLANs allowed on the trunk. The **add**, **except**, **none**, or **remove** keywords specify the action to take for the specified VLANs.
- ```
Router(config-if)# switchport trunk allowed vlan add vlan1, vlan2, vlan3
```



**Note** All VLANs are allowed by default. You cannot remove any of the default VLANs from a trunk.

---

**Step 8** Activate the interface.

```
Router(config-if) # no shutdown
```

**Step 9** Exit configuration mode.

```
Router(config-if) # end
Router#
```

You can use the `show running-configuration` command to verify the layer 2 trunk configuration.

---

## Configuring a Layer 2 Interface as Layer 2 Access

Follow these steps below to configure a Fast Ethernet interface as Layer 2 access.

---

**Step 1** Enter enable mode.

```
Router> enable
Router#
```

**Step 2** Enter configuration mode.

```
Router# configure terminal
Router(config)#
```

**Step 3** Enter configuration for the interface that you want to modify.

```
Router(config)# interface gigabitethernet 0/1
Router(config-if)#
```

**Step 4** Shut down the interface.

```
Router(config-if) # shutdown
```

**Step 5** Use the `switchport mode access` command to configure the interface as a Layer 2 access.

```
Router(config-if) # switchport mode trunk
```

Use the `switchport access vlan` command to specify an access VLAN for access ports.

```
Router(config-if) # switchport access vlan 1
```

**Step 6** Activate the interface.

```
Router(config-if) # no shutdown
```

**Step 7** Exit configuration mode.

```
Router(config-if) # end
Router#
```

You can use the `show running-config interface` command and the `show interfaces` command to verify layer 2 access configuration.

---



## Configuring HWIC-9ESW Interfaces

For instructions on how to configure stacking on the HWIC-9ESW card, see the [“Configuring Stacking” section on page 4-11](#). For more information about how to configure other features on the HWIC-D-9ESW Card, see the [“Configuring Layer 2 Interfaces” section on page 4-6](#).

### Configuring Stacking

Stacking allows two switch modules to behave as a single switch. Follow these steps to configure stacking for the HWIC-9ESW card.

- Step 1** Enter configuration mode for FastEthernet port 8 of the HWIC-9ESW card.

```
Router(config)# interface FastEthernet1/8
```



**Note** You must use FastEthernet port 8 as the stacking port.

- Step 2** Use the **no shutdown** command to bring the interface to an active state.

```
Router(config)# no shutdown
```



**Note** The line protocol state of the stacking port interface displays as down when in use.

- Step 3** Use the **switchport stacking-partner** command to specify the GigabitEthernet port that the HWIC-9ESW FastEthernet port uses as a stacking partner.

```
router(config-if)# switchport stacking-partner interface GigabitEthernet0/2
```

- Step 4** Enter the **exit** command to exit the FastEthernet interface configuration.

```
Router(config-if)# exit  
Router(config)#
```

- Step 5** Enter configuration mode for the GigabitEthernet port that you want to use as a stacking partner.

```
Router(config)# interface GigabitEthernet0/2
```

- Step 6** Use the **no shutdown** command to bring the interface to an active state.

```
Router(config)# no shutdown
```



**Note** Once you configure the FastEthernet port as a stacking partner, the corresponding GigabitEthernet interface is automatically configured as a stacking partner.

- Step 7** Connect a crossover Ethernet cable from FastEthernet port 8 of the HWIC-9ESW card to the GigabitEthernet port that you want to use as a stacking partner.

**Note**

For more detailed instructions, see the *Cisco MWR 2941-DC Mobile Wireless Edge Router Hardware Installation Guide*.

## Configuring VLANs

The Cisco MWR 2941 router supports a full set of VLAN features. You can create a maximum of 255 VLANs on the Cisco MWR 2941. The following sections describe how to configure VLANs.

- [Adding a VLAN Instance](#)
- [Deleting a VLAN Instance](#)
- [Configuring VLAN Trunking Protocol](#)

### Adding a VLAN Instance

Follow these steps to add a VLAN instance.

- 
- Step 1** Enter enable mode.
- ```
Router> enable
Router#
```
- Step 2** Enter configuration mode.
- ```
Router# configure terminal
Router(config)#
```
- Step 3** Use the **vlan** command to add a new VLAN.
- ```
Router(config)# vlan 2
```
- Step 4** Exit configuration mode.
- ```
Router(config)# exit
Router#
```
- 

### Deleting a VLAN Instance

Follow these steps to delete a VLAN from the database.

**Note**

You cannot delete Ethernet VLAN 1 and FDDI and Token Ring VLANs 1002 to 1005.

- 
- Step 1** Enter enable mode.
- ```
Router> enable
Router#
```

- Step 2** Enter configuration mode.
- ```
Router# configure terminal  
Router(config)#
```
- Step 3** Use the **no vlan** command to delete an VLAN from the database.
- ```
Router(config)# no vlan 1
```
- Step 4** Exit configuration mode.
- ```
Router(config)# exit  
Router#
```
- 

## Configuring VLAN Trunking Protocol

This section describes how to configure the VLAN Trunking Protocol (VTP) on an EtherSwitch HWIC, and contains the following tasks:

- [Configuring a VTP Server](#)
- [Configuring a VTP Client](#)
- [Disabling VTP](#)

### Configuring a VTP Server

When a switch is in VTP server mode, you can change the VLAN configuration and have it propagate throughout the network. Follow these steps to configure the switch as a VTP server.

- 
- Step 1** Enter enable mode.
- ```
Router> enable  
Router#
```
- Step 2** Enter configuration mode.
- ```
Router# configure terminal  
Router(config)#
```
- Step 3** Use the **vtp mode server** command to configure the switch as a VTP server.
- ```
Router(config)# vtp mode server
```
- Step 4** Use the **vtp domain** command to defines the VTP domain name, which can be up to 32 characters long.
- ```
Router(config)# vtp domain distantusers
```
- Step 5** If you want to specify a password for the VTP domain, use **vtp password** command. The password can be from 8 to 64 characters long. This step is optional.
- ```
Router(config)# vtp password philadelphia
```
- Step 6** Exit configuration mode.
- ```
Router(config)# exit  
Router#
```
-

## Configuring a VTP Client

When a switch is in VTP client mode, you cannot change the VLAN configuration on the switch. The client switch receives VTP updates from a VTP server in the management domain and modifies its configuration accordingly. Follow these steps to configure a VTP client.

- 
- Step 1** Enter enable mode.
- ```
Router> enable
Router#
```
- Step 2** Enter configuration mode.
- ```
Router# configure terminal
Router(config)#
```
- Step 3** Use the **vtp mode client** command to configure the switch as a VTP client.
- ```
Router(config)# vtp mode client
```
- Step 4** Exit configuration mode.
- ```
Router(config)# exit
Router#
```
- 

## Disabling VTP

You can disable VTP on a switch by configuring it to VTP transparent mode, meaning that the switch does not send VTP updates or act on VTP updates received from other switches. Follow these steps to disable VTP on the switch.

- 
- Step 1** Enter enable mode.
- ```
Router> enable
Router#
```
- Step 2** Enter configuration mode.
- ```
Router# configure terminal
Router(config)#
```
- Step 3** Use the **vtp mode transparent** command to set the switch in VTP transparent mode.
- ```
Router(config)# vtp mode transparent
```
- Step 4** Exit configuration mode.
- ```
Router(config)# exit
Router#
```

**Note**

You can use the **show vtp status** command to verify the VTP status of the switch.

---

## Configuring Resilient Ethernet Protocol (REP)

A segment is a collection of ports connected one to the other in a chain and configured with a segment ID. To configure REP segments, you configure the REP administrative VLAN (or use the default VLAN 1) and then add the ports to the segment using interface configuration mode. You should configure two edge ports in the segment, one as the primary edge port and the other, by default, the secondary edge port. A segment has only one primary edge port. If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one to serve as the segment primary edge port. You can also optionally configure where to send segment topology change notices (STCNs) and VLAN load balancing messages.

The following sections describe how to configure REP on the Cisco MWR 2941.

- [Default REP Configuration, page 4-15](#)
- [REP Configuration Guidelines, page 4-15](#)
- [Configuring the REP Administrative VLAN, page 4-16](#)
- [Configuring REP Interfaces, page 4-17](#)
- [Setting Manual Preemption for VLAN Load Balancing, page 4-19](#)
- [Configuring SNMP Traps for REP, page 4-19](#)

### Default REP Configuration

REP is disabled on all interfaces. When enabled, the interface is a regular segment port unless it is configured as an edge port.

When REP is enabled, the sending of segment topology change notices (STCNs) is disabled, all VLANs are blocked, and the administrative VLAN is VLAN 1.

When VLAN load balancing is enabled, the default is manual preemption with the delay timer disabled. If VLAN load balancing is not configured, the default after manual preemption is to block all VLANs at the primary edge port.

### REP Configuration Guidelines

Follow these guidelines when configuring REP:

- We recommend that you begin by configuring one port and then configure the contiguous ports to minimize the number of segments and the number of blocked ports.
- If more than two ports in a segment fail when no external neighbors are configured, one port goes into a forwarding state in order to help maintain connectivity for the data path during configuration.
- The **show rep interface** command output displays the Port Role of each port on the router. The Port Role of ports in a forwarding state is displayed as *Fail Logical Open*; the Port Role of other failed ports is displayed as *Fail No Ext Neighbor*. When the external neighbors for the failed ports are restored, the ports go through the alternate port state transitions and eventually go to an open state or remain as the alternate port, based on the alternate port election mechanism.
- REP ports must be Layer 2 trunk ports.
- Be careful when configuring REP through a Telnet connection. Because REP blocks all VLANs until another REP interface sends a message to unblock the VLAN, you might lose connectivity to the router if you enable REP in a Telnet session that accesses the router through the REP interface.
- You cannot run REP and STP or REP and Flex Links on the same segment or interface.

- If you connect an STP network to the REP segment, be sure that the connection is at the segment edge. An STP connection that is not at the edge could cause a bridging loop because STP does not run on REP segments. All STP BPDUs are dropped at REP interfaces.
- You must configure all trunk ports in the segment with the same set of allowed VLANs, or a misconfiguration occurs.
- REP ports follow these rules:
  - There is no limit to the number of REP ports on a switch; however, only two ports on a switch can belong to the same REP segment.
  - If only one port on a switch is configured in a segment, the port should be an edge port.
  - If two ports on a switch belong to the same segment, they must be both edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and regular segment port on a switch cannot belong to the same segment.

**Note**

Release 12.2(33)MRA does not support the **no-neighbor** keyword.

- If two ports on a switch belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.
- REP interfaces come up and remain in a blocked state until notified that it is safe to unblock. You need to be aware of this to avoid sudden connection losses.
- REP sends all LSL PDUs in untagged frames on the native VLAN. The BPA message sent to the Cisco multicast address is sent on the administration VLAN, which is VLAN 1 by default.
- REP ports cannot be configured as one of these port types:
  - SPAN destination port
  - Private VLAN port
  - Tunnel port
  - Access port
- REP is supported on EtherChannels, but not on an individual port that belongs to an EtherChannel.
- There is a maximum of 64 REP segments per switch.

## Configuring the REP Administrative VLAN

To avoid the delay introduced by relaying messages in software for link-failure or VLAN-blocking notification during load balancing, REP floods packets at the hardware flood layer (HFL) to a regular multicast address. These messages are flooded to the whole network, not just the REP segment. You can control flooding of these messages by configuring an administrative VLAN for the whole domain.

Follow these guidelines when configuring the REP administrative VLAN:

- If you do not configure an administrative VLAN, the default is VLAN 1.
- There can be only one administrative VLAN on a switch and on a segment. However, this is not enforced by software.
- The administrative VLAN cannot be the RSPAN VLAN.

Beginning in privileged EXEC mode, follow these steps to configure the REP administrative VLAN:

- 
- Step 1** Enter enable mode.

```
Router> enable
```

- Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

- Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

- Step 4** Use the **rep admin vlan** command to specify the REP administrative VLAN. Valid values are 2–4094, and the default value is VLAN 1. To set the admin VLAN to 1, enter the **no rep admin vlan** global configuration command.

```
Router(config)# rep admin vlan 100
```

- Step 5** Use the **exit** command to exit configuration mode.

```
Router(config)# exit  
Router#
```

You can use the **show interface [interface-id] rep detail** command to verify your configuration.

---

## Configuring REP Interfaces

For REP operation, you need to enable it on each segment interface and to identify the segment ID. This step is required and must be done before other REP configuration. You must also configure a primary and secondary edge port on each segment. All other steps are optional.

Beginning in privileged EXEC mode, follow these steps to enable and configure REP on an interface:

- 
- Step 1** Enter enable mode.

```
Router> enable
```

- Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

- Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

- Step 4** Use the **interface** command to specify the interface you wish to configure.

```
Router(config)# interface gigabitethernet 0/2  
Router(config-if)#
```

- Step 5** Use the **switchport mode trunk** command to configure the interface as a Layer 2 trunk port.

```
Router(config-if)# switchport mode trunk
```

- Step 6** Use the **rep segment** *segment-id* to enable REP on the interface, and identify a segment number. The segment ID range is from 1 to 1024. These optional keywords are available:

- **edge**—Configures the port as an edge port.
- **primary**—Configures an edge port as the primary edge port
- **preferred**—Sets the port as the preferred alternate port or the preferred port for VLAN load balancing.

```
Router(config-if)# rep segment 100 edge primary
```

For more information about the syntax for this command, see the [Appendix B, “Cisco MWR 2941 Router Command Reference.”](#)

- Step 7** Use the **rep stcn** command to configure the edge port to send segment topology change notices (STCNs). This command has the following parameters:

- **interface** *interface-id*—Designates a physical interface or port channel to receive STCNs.
- **segment** *id-list*—Identifies one or more segments to receive STCNs. The range is 1 to 1024.
- **stp**—Sends STCNs to STP networks.

```
Router(config-if)# rep stcn interface gigabitethernet0/2 segment 500 stp
```

- Step 8** Use the **rep block port** command to configure VLAN load balancing on the primary edge port, identify the REP alternate port, and configure the VLANs to be blocked on the alternate port.

- **id** *port-id*—Identifies the alternate port by port ID. The port ID is automatically generated for each port in the segment. You can view interface port IDs by entering the **show interface interface-id rep [detail]** privileged EXEC command.
- **neighbor\_offset**—Identifies the alternate port as a downstream neighbor from an edge port. The range is from -256 to 256, with negative numbers identifying the downstream neighbor from the secondary edge port. A value of 0 is invalid. Enter -1 to identify the secondary edge port as the alternate port. See [Figure 1-4 on page 1-8](#) for an example of neighbor offset numbering.



#### Note

Because you enter this command at the primary edge port (offset number 1), you would never enter an offset value of 1 to identify an alternate port.

- **preferred**—Selects the regular segment port previously identified as the preferred alternate port for VLAN load balancing.
- **vlan** *vlan-list*—Blocks one VLAN or a range of VLANs.
- **vlan all**—Blocks all VLANs.



#### Note

Enter this command only on the REP primary edge port.

```
Router(config-if)# rep block port 0009001818D68700 vlan all
```

- Step 9** Use the **rep preempt delay** *seconds* command to configure a preempt time delay if you want VLAN load balancing to automatically trigger after a link failure and recovery. The time delay range is 15 to 300 seconds. The default is manual preemption with no time delay. This command only applies to the REP primary edge port.



```
Router(config-if)# rep preempt delay 60
```

- Step 10** Exit configuration mode.

```
Router(config-if)# end  
Router#
```

You can use the **show interface** *[interface-id]* **rep detail** command to verify your configuration. Enter the **show rep topology** command to see which port in the segment is the primary edge port.

---

## Setting Manual Preemption for VLAN Load Balancing

If you do not enter the **rep preempt delay** *seconds* command on the primary edge port to configure a preemption time delay, the default setting is to manually trigger VLAN load balancing on the segment. Be sure to complete all other segment configuration before manually preempting VLAN load balancing. When you enter the **rep preempt segment** *segment-id* command, a confirmation message appears before the command is executed because preemption can cause network disruption.

Beginning in privileged EXEC mode, follow these steps on the switch that has the segment primary edge port to manually trigger VLAN load balancing on a segment:

- Step 1** Use the **rep preempt segment** command to manually trigger VLAN load balancing on the segment. You need to confirm the command before it is executed.

```
Router# rep preempt segment segment-id
```

- Step 2** Use the **show rep topology** command to view REP topology information.

```
Router# show rep topology
```

---

## Configuring SNMP Traps for REP

You can configure the switch to send REP-specific traps to notify the SNMP server of link operational status changes and port role changes. Beginning in privileged EXEC mode, follow these steps to configure REP traps:

- Step 1** Enter enable mode.

```
Router> enable
```

- Step 2** Enter the password.

```
Password: password
```

When the prompt changes to *Router*, you have entered enable mode.

- Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

- Step 4** Use the **snmp mib rep trap-rate** command to enable the switch to send REP traps and set the number of traps sent per second. The range is from 0 to 1000. The default is 0 (no limit imposed; a trap is sent at every occurrence).

```
Router(config)# snmp mib rep trap-rate 10
```

**Step 5** Exit configuration mode.

```
Router(config)# end
Router#
```

You can use the **show running-config** command to verify your configuration.

## Monitoring REP

You can use the following commands to monitor REP.

- **show interface [interface-id] rep [detail]**—Displays REP configuration and status for a specified interface or for all interfaces. The following example shows sample output for this command.

```
Router# show interface gigabitethernet0/0 rep
Interface                Seg-id Type          LinkOp    Role
-----
GigabitEthernet0/0      2          TWO_WAY   Open

sh int gig0/0 rep detail
GigabitEthernet0/0    REP enabled
Segment-id: 2 (Segment)
PortID: 0001002255000284
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 05020014A91176C0B1C0
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none Configured Load-balancing Block VLAN: none
STCN Propagate to: none LSL PDU rx: 239621, tx: 183515 HFL PDU rx: 9, tx: 1 BPA TLV
rx: 86252, tx: 11033 BPA (STCN, LSL) TLV rx: 0, tx: 0 BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 39, tx: 82 EPA-COMMAND TLV rx: 0, tx: 0 EPA-INFO TLV rx: 19037,
tx: 19075
```

- **show rep topology [segment segment\_id] [archive] [detail]**—Displays REP topology information for a segment or for all segments, including the primary and secondary edge ports in the segment. The following example shows sample output for this command.

```
Router# show rep topology segment 2
REP Segment 2
BridgeName      PortName      Edge Role
-----
switch1         Gi6/2         Pri  Alt
switch3         Gi0/1         Open
switch3         Gi0/0         Open
switch2         Gi0/0         Open
switch2         Gi0/1         Open
switch4         Gi0/0         Open
switch4         Gi0/3         Open
switch5         Gi0/11        Sec  Open
```

## Configuring Ethernet Connectivity Fault Management (CFM)

Ethernet Connectivity Fault Management (CFM) is an end-to-end per-service-instance Ethernet layer operations, administration, and maintenance (OAM) protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs. Ethernet CFM provides a competitive advantage to service providers in managing link uptime and isolating and responding to network failures.

The following sections describe how to set up Ethernet CFM on the Cisco MWR 2941:

- [Understanding Ethernet CFM](#)
- [Configuring Ethernet CFM](#)

### Understanding Ethernet CFM

Before you set up Ethernet CFM, you should understand the following concepts:

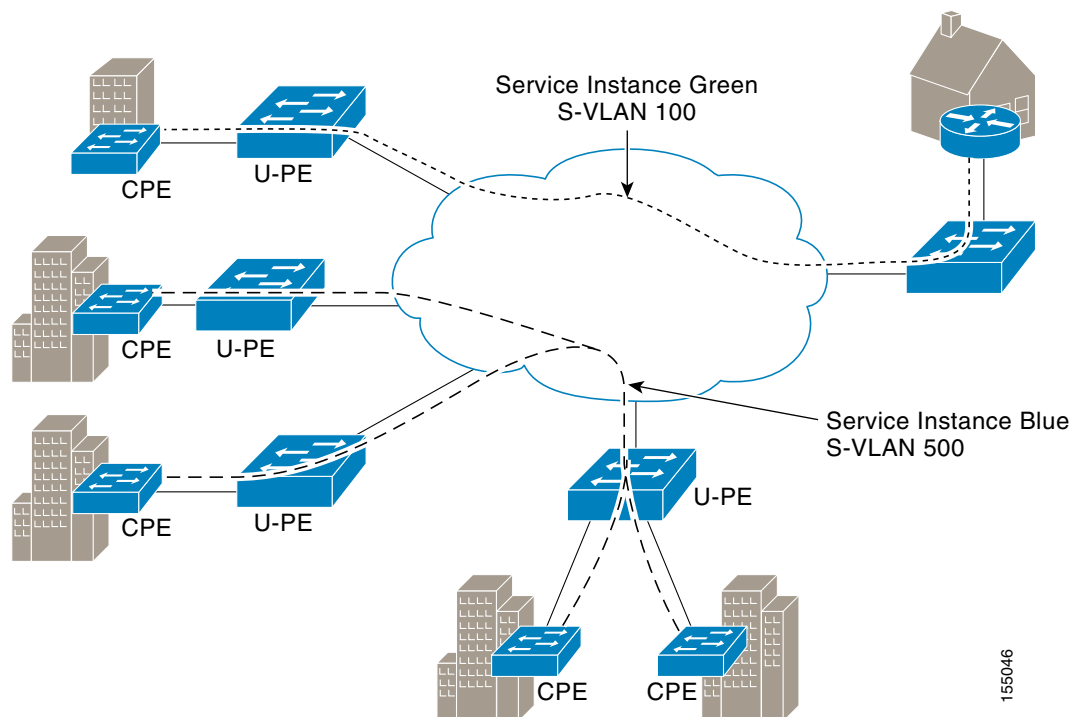
- [Customer Service Instance, page 4-21](#)
- [Maintenance Domain, page 4-22](#)
- [Maintenance Point, page 4-24](#)
- [CFM Messages, page 4-26](#)
- [Cross-Check Function, page 4-27](#)
- [SNMP Traps, page 4-28](#)
- [Ethernet CFM and Ethernet OAM Interaction, page 4-28](#)
- [NSF/SSO Support in CFM 802.1ag/1.0d, page 4-29](#)
- [NSF/SSO Support in CFM 802.1ag/1.0d, page 4-29](#)
- [ISSU Support in CFM 802.1ag/1.0d, page 4-29](#)

**Note**

For additional information about Ethernet CFM, see the [Cisco IOS Carrier Ethernet Configuration Guide, Release 12.2SR](#).

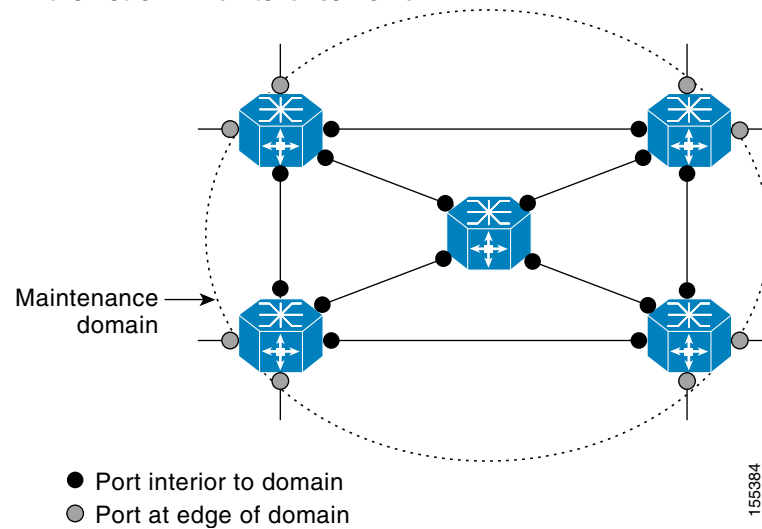
### Customer Service Instance

A customer service instance is an Ethernet virtual connection (EVC), which is identified by an S-VLAN within an Ethernet island and a globally unique service ID. A customer service instance can be point-to-point or multipoint-to-multipoint. [Figure 4-1](#) shows two customer service instances. Service Instance Green is point to point; Service Instance Blue is multipoint to multipoint.

**Figure 4-1** *Customer Service Instances*

## Maintenance Domain

Maintenance domains define portions of a service provider network according to network management requirements and determine how CFM functions within the network. A domain is owned and operated by a single entity and defined by the set of ports internal to it and at its boundary. [Figure 4-2](#) illustrates a typical maintenance domain.

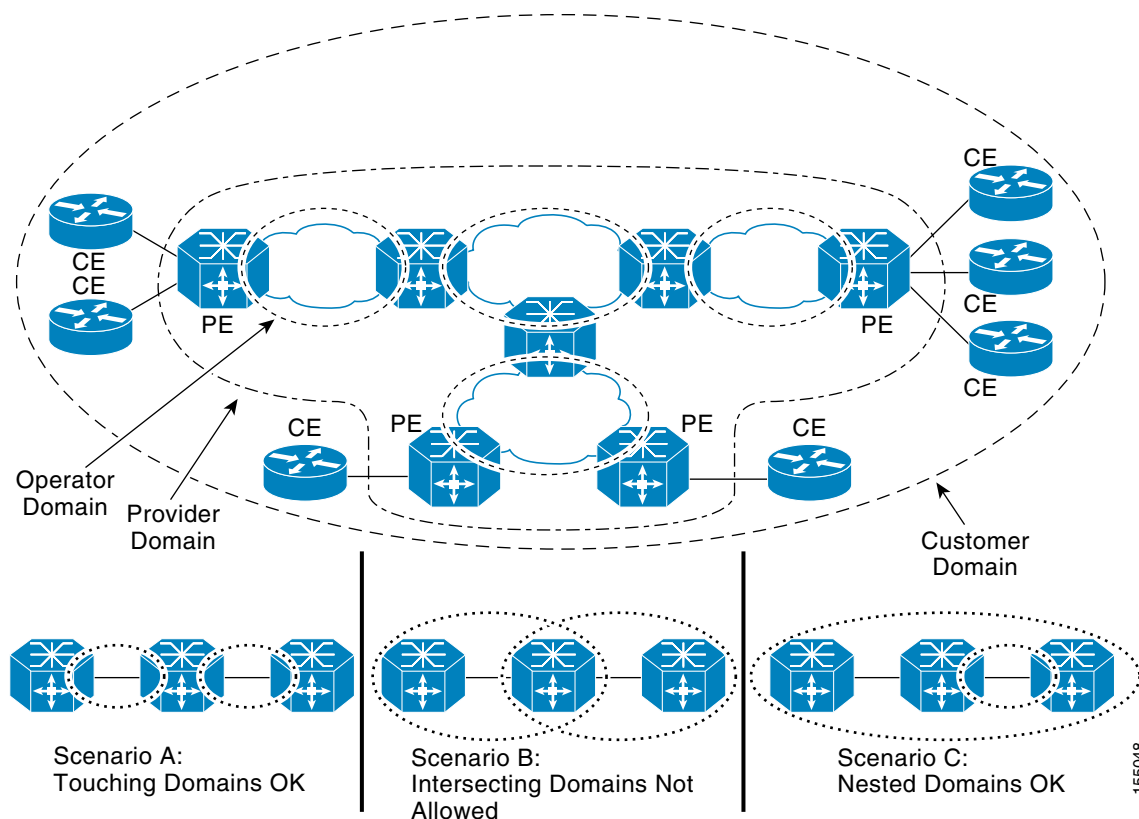
**Figure 4-2 Ethernet CFM Maintenance Domain**

A unique maintenance level in the range of 0 to 7 is assigned to each domain by a network administrator. Levels and domain names are useful for defining the hierarchical relationship that exists among domains. The hierarchical relationship of domains parallels the structure of customer, service provider, and operator. The larger the domain, the higher the level value. For example, a customer domain would be larger than an operator domain. The customer domain may have a maintenance level of 7 and the operator domain may have a maintenance level of 0. Typically, operators would have the smallest domains and customers the largest domains, with service provider domains between them in size. All levels of the hierarchy must operate together.

Domains should not intersect because intersecting would mean management by more than one entity, which is not allowed. Domains may nest or touch but when two domains nest, the outer domain must have a higher maintenance level than the domain nested within it. Nesting maintenance domains is useful in the business model where a service provider contracts with one or more operators to provide Ethernet service to a customer. Each operator would have its own maintenance domain and the service provider would define its domain—a superset of the operator domains. Furthermore, the customer has its own end-to-end domain which is in turn a superset of the service provider domain. Maintenance levels of various nesting domains should be communicated among the administering organizations. For example, one approach would be to have the service provider assign maintenance levels to operators.

CFM exchanges messages and performs operations on a per-domain basis. For example, running CFM at the operator level does not allow discovery of the network by the higher provider and customer levels.

Network designers decide on domains and configurations. [Figure 4-3](#) illustrates a hierarchy of operator, service provider, and customer domains and also illustrates touching, intersecting, and nested domains.

**Figure 4-3 Ethernet CFM Maintenance Domain Hierarchy**

## Maintenance Point

A maintenance point is a demarcation point on an interface (port) that participates in CFM within a maintenance domain. Maintenance points on device ports act as filters that confine CFM frames within the bounds of a domain by dropping frames that do not belong to the correct level. Maintenance points must be explicitly configured on Cisco devices. Two classes of maintenance points exist, MEPs and MIPs.

### Maintenance Endpoints (MEPs)

MEPs have the following characteristics:

- Per maintenance domain (level) and service (S-VLAN or EVC)
- At the edge of a domain, define the domain boundary
- Confine CFM messages within the bounds of a maintenance domain,
- Can proactively transmit CFM continuity check messages (CCMs)
- Can transmit traceroute and loopback messages at administrator request

### Inward Facing MEPs

*Inward facing* means the MEP communicates through the Bridge Relay function and uses the Bridge-Brain MAC address. An inward facing MEP performs the following functions:

- Sends and receives CFM frames at its level through the relay function, not via the wire connected to the port on which the MEP is configured.
- Drops all CFM frames at its level (or lower level) that come from the direction of the wire.

- Processes all CFM frames at its level coming from the direction of the relay function.
- Drops all CFM frames at a lower level coming from the direction of the relay function.
- Transparently forwards all CFM frames at its level (or a higher level), independent of whether they come in from the relay function side or the wire side.



**Note** For the current Cisco IOS implementation, a MEP of level L (where L is less than 7) requires a MIP of level M > L on the same port; hence, CFM frames at a level higher than the level of the MEP are catalogued by this MIP.

- If the port on which the inward MEP is configured is blocked by Spanning-Tree Protocol, the MEP can no longer transmit or receive CFM messages.

### Outward Facing MEPs for Routed Ports and Switch Ports

*Outward facing* means that the MEP communicates through the wire. Outward facing MEPs can be configured on routed ports and switch ports. A MIP configuration at a level higher than the level of the outward facing MEP is not required.

Outward facing MEPs on routed ports use the port MAC address. Outward facing MEPs on port channels use the Bridge-Brain MAC address of the first member link. When port channel members change, the identities of outward facing MEPs do not have to change. Cisco IOS Release 12.2(33)MRA supports outward facing MEPs on switch ports and Ethernet flow points (EFPs).

An outward facing MEP performs the following functions:

- Sends and receives CFM frames at its level via the wire connected to the port where the MEP is configured.
- Drops all CFM frames at its level (or at a lower level) that come from the direction of the relay function.
- Processes all CFM frames at its level coming from the direction of the wire.
- Drops all CFM frames at a lower level coming from the direction of the wire.
- Transparently forwards all CFM frames at levels higher than the level of the outward facing MEP, independent of whether they come in from the relay function side or the wire side. This function is not applicable to routed ports.

If the port on which the outward MEP is configured is blocked by Spanning-Tree Protocol, the MEP can still transmit and receive CFM messages via the wire. Cisco IOS Release 12.2(33)MRA does not support CFM messages passing through a blocked port.

### Maintenance Intermediate Points

MIPs have the following characteristics:

- Act on a maintenance domain (level) and for all S-VLANs that are enabled or allowed on a port.
- Are internal to a domain, not at the boundary.
- Passive points respond only when triggered by CFM traceroute and loopback messages.
- Use Bridge-Brain MAC addresses.
- Handle CFM as follows:
  - CFM frames received from MEPs and other MIPs are catalogued and forwarded, using both the wire and the relay function.

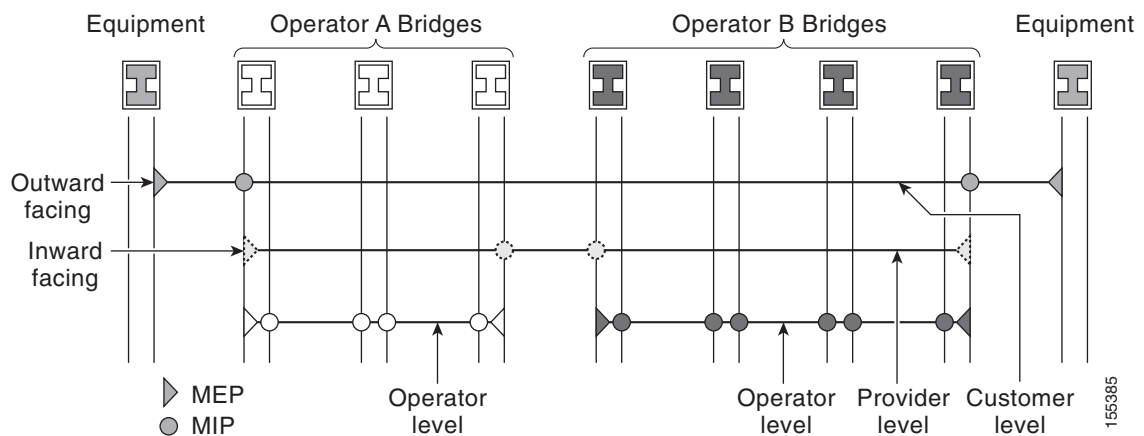
- All CFM frames at a lower level are stopped and dropped, independent of whether they originate from the wire or relay function.
- All CFM frames at a higher level are forwarded, independent of whether they arrive from the wire or relay function.

If the port on which a MIP is configured is blocked by Spanning-Tree Protocol, the MIP cannot receive CFM messages or relay them toward the relay function side. The MIP can, however, receive and respond to CFM messages from the wire.

A MIP has only one level associated with it and the command-line interface (CLI) does not allow you to configure a MIP for a domain that does not exist.

Figure 4-4 illustrates MEPs and MIPs at the operator, service provider, and customer levels.

**Figure 4-4 CFM MEPs and MIPs on Customer and Service Provider Equipment, Operator Devices**



## CFM Messages

CFM uses standard Ethernet frames. CFM frames are distinguishable by EtherType and for multicast messages by MAC address. CFM frames are sourced, terminated, processed, and relayed by bridges. Routers can support only limited CFM functions.

Bridges that cannot interpret CFM messages forward them as normal data frames. All CFM messages are confined to a maintenance domain and to an S-VLAN (PE-VLAN or Provider-VLAN). Three types of messages are supported:

- Continuity Check
- Loopback
- Traceroute



### Continuity Check Messages

CFM CCMs are multicast heartbeat messages exchanged periodically among MEPs. They allow MEPs to discover other MEPs within a domain and allow MIPs to discover MEPs. CCMs are confined to a domain and S-VLAN.

CFM CCMs have the following characteristics:

- Transmitted at a configurable periodic interval by MEPs. The interval can be from 10 seconds to 65535 seconds, the default is 30.
- Contain a configurable hold-time value to indicate to the receiver the validity of the message. The default is 2.5 times the transmit interval.
- Catalogued by MIPs at the same maintenance level.
- Terminated by remote MEPs at the same maintenance level.
- Unidirectional and do not solicit a response.
- Carry the status of the port on which the MEP is configured.

### Loopback Messages

CFM loopback messages are unicast frames that a MEP transmits, at the request of an administrator, to verify connectivity to a particular maintenance point. A reply to a loopback message indicates whether a destination is reachable but does not allow hop-by-hop discovery of the path. A loopback message is similar in concept to an Internet Control Message Protocol (ICMP) Echo (ping) message.

A CFM loopback message can be generated on demand using the CLI. The source of a loopback message must be a MEP; the destination may be a MEP or a MIP. CFM loopback messages are unicast; replies to loopback messages also are unicast. CFM loopback messages specify the destination MAC address, VLAN, and maintenance domain.

### Traceroute Messages

CFM traceroute messages are multicast frames that a MEP transmits, at the request of an administrator, to track the path (hop-by-hop) to a destination MEP. They allow the transmitting node to discover vital connectivity data about the path, and allow the discovery of all MIPs along the path that belong to the same maintenance domain. For each visible MIP, traceroute messages indicate ingress action, relay action, and egress action. Traceroute messages are similar in concept to User Datagram Protocol (UDP) traceroute messages.

Traceroute messages include the destination MAC address, VLAN, and maintenance domain and they have Time To Live (TTL) to limit propagation within the network. They can be generated on demand using the CLI. Traceroute messages are multicast; reply messages are unicast.

## Cross-Check Function

The cross-check function is a timer-driven post-provisioning service verification between dynamically discovered MEPs (via CCMs) and expected MEPs (via configuration) for a service. The cross-check function verifies that all endpoints of a multipoint or point-to-point service are operational. The function supports notifications when the service is operational; otherwise it provides alarms and notifications for unexpected endpoints or missing endpoints.

The cross-check function is performed one time. You must initiate the cross-check function from the CLI every time you want a service verification.

## SNMP Traps

The support provided by the Cisco IOS software implementation of CFM traps is Cisco proprietary information. MEPs generate two types of Simple Network Management Protocol (SNMP) traps, continuity check (CC) traps and cross-check traps.

### CC Traps

- MEP up—Sent when a new MEP is discovered, the status of a remote port changes, or connectivity from a previously discovered MEP is restored after interruption.
- MEP down—Sent when a timeout or last gasp event occurs.
- Cross-connect—Sent when a service ID does not match the VLAN.
- Loop—Sent when a MEP receives its own CCMs.
- Configuration error—Sent when a MEP receives a continuity check with an overlapping MPID.

### Cross-Check Traps

- Service up—Sent when all expected remote MEPs are up in time.
- MEP missing—Sent when an expected MEP is down.
- Unknown MEP—Sent when a CCM is received from an unexpected MEP.

## Ethernet CFM and Ethernet OAM Interaction

To understand how CFM and OAM interact, you should understand the following concepts:

- [Ethernet Virtual Circuit, page 4-28](#)
- [OAM Manager, page 4-28](#)
- [CFM over Bridge Domains, page 4-29](#)

### Ethernet Virtual Circuit

An EVC as defined by the Metro Ethernet Forum is a port-level point-to-point or multipoint-to-multipoint Layer 2 circuit. EVC status can be used by a CE device to find an alternative path to the service provider network or fall back to a backup path over Ethernet or over another alternative service such as ATM.

**Note**

---

Release 12.2(33)MRA does not support configuration of EVCs; it can only receive EVC status information as a CE device.

---

### OAM Manager

The OAM manager is an infrastructure element that streamlines interaction between OAM protocols. The OAM manager requires two interworking OAM protocols, in this case Ethernet CFM and Ethernet OAM. Interaction is unidirectional from the OAM manager to the CFM protocol and the only information exchanged is the user network interface (UNI) port status. Additional port status values available include

- REMOTE\_EE—Remote excessive errors
- LOCAL\_EE—Local excessive errors
- TEST—Either remote or local loopback

After CFM receives the port status, it communicates that status across the CFM domain.

### CFM over Bridge Domains

The Ethernet OAM 3.0—CFM over BD, Untagged feature allows untagged CFM packets to be associated with a MEP. An incoming untagged customer CFM packet has an EtherType of CFM and is mapped to an EVC or bridge domain (BD) based on the encapsulation configured on the EFP. The EFP is configured specifically to recognize these untagged packets.

An EFP is a logical demarcation point of an EVC on an interface and can be associated with a bridge domain. The VLAN ID is used to match and map traffic to the EFP. VLAN IDs have local significance per port similar to ATM/FrameRelay virtual circuits. CFM is supported on a bridge domain associated with an EFP. The association between the bridge domain and the EFP allows CFM to use the encapsulation on the EFP. All EFPs in the same bridge domain form a broadcast domain. The bridge domain ID determines the broadcast domain.

The distinction between a VLAN port and the EFP is the encapsulation. VLAN ports use a default dot1q encapsulation. For EFPs, untagged, single tagged, and double tagged encapsulation exists with dot1q and IEEE dot1ad EtherTypes. Different EFPs belonging to the same bridge domain can use different encapsulations.

**Note**

The Ethernet OAM 3.0—CFM over BD, Untagged feature is supported only on ES20 and ES40 line cards.

### NSF/SSO Support in CFM 802.1ag/1.0d

The redundancy configurations SSO and NSF are both supported in Ethernet CFM and are automatically enabled. A switchover from an active to a standby RP occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance. NSF interoperates with the SSO feature to minimize network downtime following a switchover. The primary function of Cisco NSF is to continue forwarding IP packets following an RP switchover.

For detailed information about SSO, see the “Stateful Switchover” chapter of the [Cisco IOS High Availability Configuration Guide](#). For detailed information about the NSF feature, see the “Cisco Nonstop Forwarding” chapter of the [Cisco IOS High Availability Configuration Guide](#).

### ISSU Support in CFM 802.1ag/1.0d

ISSU allows you to perform a Cisco IOS software upgrade or downgrade without disrupting packet flow. CFM performs a bulk update and a runtime update of the continuity check database to the standby RP, including adding, deleting, or updating a row. This checkpoint data requires ISSU capability to transform messages from one release to another. All the components that perform active RP to standby RP updates using messages require ISSU support.

ISSU is automatically enabled in CFM and lowers the impact that planned maintenance activities have on network availability by allowing software changes while the system is in service. For detailed information about ISSU, see the “Cisco IOS In Service Software Upgrade Process” chapter of the [Cisco IOS High Availability Configuration Guide](#).

## Configuring Ethernet CFM

The following sections describe how to configure Ethernet CFM.

- [Configuring Global settings](#)
- [Configuring and Enabling the Cross-Check Function](#)
- [Configuring Ethernet Link Operations, Administration, and Maintenance \(OAM\)](#)

**Note**

For additional information about Ethernet CFM, see the [Cisco IOS Carrier Ethernet Configuration Guide, Release 12.2SR](#).

### Configuring Global settings

- Step 1** Use the **ethernet cfm enable** command to enable Ethernet CFM.

**Note**

Release 12.2(33)MRA supports the Draft 1.0 version of Ethernet CFM; it does not support the IEEE 802.1ag-2007 version.

```
Router(config)# ethernet cfm enable
```

- Step 2** Follow these steps to configure an Ethernet CFM domain.

- a.** Use the **ethernet cfm domain** command to define a CFM maintenance domain at a particular maintenance level and enter Ethernet CFM configuration mode.

```
Router(config)# ethernet cfm domain CUST_L6 level 6
Router(config-ether-cfm)#
```

- b.** Use the **mep archive-hold-time** command to set the amount of time, in minutes, that data from a missing maintenance end point (MEP) is kept in the continuity check database or that entries are held in the error database before they are purged.

```
Router(config-ether-cfm)# mep archive-hold-time 1000
```

- c.** Use the **service** command to configure a maintenance association within a maintenance domain and enter connectivity fault management (CFM) service configuration mode. You can use the following parameters:

- **ma-name**—The maintenance association ID (MAID) is a combination of a maintenance domain ID and the short maintenance association name.
- **ma-num**—Integer from 0 to 65535 that identifies the maintenance association.
- **vlan-id**—Configures a primary VLAN.
- **vpn-id**—Configures a virtual private network (VPN).

```
Router(config-ether-cfm)# service CE_600 vlan 600
```

Repeat this step to define multiple services within a single domain.

- d.** Exit CFM service configuration mode.

```
Router(config-ether-cfm)# exit
Router(config)#
```

- e.** Repeat steps 1–3 to create additional CFM maintenance domains.

- Step 3** Use the **ethernet cfm enable** command to enables CFM processing globally on the router.
- ```
Router(config)# ethernet cfm enable
```
- Step 4** Use the **ethernet cfm traceroute cache** command to enable caching of CFM data learned through traceroute messages.
- ```
Router(config)# ethernet cfm traceroute cache
```
- Step 5** Use the **ethernet cfm traceroute cache size** command to set a maximum size for the Ethernet CFM traceroute cache table.
- ```
Router(config)# ethernet cfm traceroute cache size 112
```
- Step 6** Use the **ethernet cfm traceroute cache hold-time** command to set the time that Ethernet connectivity fault management (CFM) traceroute cache entries are retained.
- ```
Router(config)# ethernet cfm traceroute cache hold-time 65535
```
- Step 7** Use the **ethernet cfm cc enable** command to globally enable transmission of continuity check messages (CCMs).
- ```
Router(config)# ethernet cfm cc enable level any vlan any
```
- Step 8** Use the **ethernet cfm cc level** command to set parameters for continuity check messages (CCMs).
- ```
Router(config)# ethernet cfm cc level any vlan any interval 20 loss-threshold 3
```
- Step 9** Use the **snmp-server enable traps ethernet cfm cc** command to enable SNMP trap generation for Ethernet CFM continuity check events.
- ```
Router(config)# snmp-server enable traps ethernet cfm cc mep-up mep-down config loop cross-connect
```
- Step 10** Use the **snmp-server enable traps ethernet cfm crosscheck** command to enable SNMP trap generation for Ethernet CFM continuity check events in relation to the cross-check operation between statically configured MEPS and those learned via CCMs.
- ```
Router(config)# snmp-server enable traps ethernet cfm crosscheck mep-unknown mep-missing service-up
```
- Step 11** Use the **ethernet lmi global** command to enable Ethernet local management interface (LMI) globally on the router.
- ```
Router(config)# ethernet lmi global
```
- Step 12** Follow these steps to configure an interface to use CFM.
- Use the **interface** command to specify an interface and enter interface configuration mode.
- ```
Router(config)# interface GigabitEthernet0/2
Router(config-if)#
```
- If you specified a VLAN ID for the CFM service, use the **switchport access vlan** command to put the interface into the VLAN.
- ```
Router(config-if)# switchport access vlan 600
```
- If you want to specify the interface as a trunking VLAN Layer 2 interface, enter the **switchport mode trunk** command.
- ```
Router(config-if)# switchport mode trunk
```
- If you set the interface in trunking mode, use the **switchport trunk native** command to set the native VLAN for the trunk.

```
Router(config-if)# switchport trunk native vlan 600
```

- d. If you want to set the port as internal to a maintenance domain and define it as a maintenance endpoint (MEP) use the **ethernet cfm mep domain mpid** command in interface configuration mode. This command enters Ethernet CFM MEP configuration mode.

```
Router(config-if)# ethernet cfm mep domain CISCO_5 mpid 529 vlan 1
```

- e. If you want to provision a maintenance intermediate point (MIP) at a specified maintenance level on the interface, use the **ethernet cfm mip level** command in interface configuration mode.

```
Router(config-if)# ethernet cfm mip level 5
```

- f. Exit interface configuration mode.

```
Router(config-if)# exit
```

- Step 13** Use the **ethernet cfm cc enable level vlan** command in global configuration mode to globally enable transmission of continuity check messages (CCMs).

```
Router(config)# ethernet cfm cc enable level 0-7 vlan 1-4094
```

For more information about how to configure CFM, see the [Cisco IOS Carrier Ethernet Configuration Guide, Release 12.2SR](#).

## Configuring and Enabling the Cross-Check Function

Follow these steps to configure and enable cross-checking for an inward facing MEP. This task requires you to configure and enable cross-checking on two devices. This task is optional.

- 
- Step 1** Enter enable mode.

```
Router> enable
```

- Step 2** Enter the password.

```
Password: password
```

When the prompt changes to *Router*, you have entered enable mode.

- Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

- Step 4** Use the **ethernet cfm domain** command to define an outward CFM domain at a specified level and enter Ethernet CFM configuration mode.

```
Router(config)# ethernet cfm domain Customer level 7 direction outward
```

- Step 5** Use the **mep crosscheck mpid** command to statically define a remote MEP on a VLAN within a specified domain.

```
Router(config-ether-cfm)# mep crosscheck mpid 401 vlan 100
```

- Step 6** Exit to global configuration mode.

```
Router(config-ether-cfm)# exit
Router(config)#
```

- Step 7** Use the **ethernet cfm mep crosscheck start-delay** command to configure the maximum amount of time that the router waits for remote MEPs to come up before starting the cross-check operation.

```
Router(config)# ethernet cfm mep crosscheck start-delay 60
```

- Step 8** Use the **ethernet cfm mep crosscheck** command to enable cross-checking between MEPs.

```
Router# ethernet cfm mep crosscheck enable level 7 vlan 100
```

## Configuring Ethernet Link Operations, Administration, and Maintenance (OAM)

The following sections describe how to configure Ethernet OAM:

- [Enabling Ethernet OAM on an Interface](#)
- [Stopping and Starting Link Monitoring Operations](#)
- [Stopping and Starting Link Monitoring Operations](#)
- [Configuring Link Monitoring Options](#)
- [Configuring Global Ethernet OAM Options Using a Template](#)

### Enabling Ethernet OAM on an Interface

Follow these steps to enable Ethernet OAM on an interface on the Cisco MWR 2941.

- Step 1** Enter enable mode.

```
Router> enable
```

- Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

- Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

- Step 4** Use the **interface** command to specify the interface you wish to configure.

```
Router(config)# interface gigabitethernet 0/2
Router(config-if)#
```

- Step 5** Use the **ethernet oam** command to enable Ethernet OAM on the interface. You can use the following parameters:

- **max-rate**—Sets the maximum rate per second for OAM PDUs.
- **min-rate**—Sets the minimum rate per second for OAM PDUs.
- **mode**—Sets the OAM client mode (active or passive).
- **timeout**—Specifies the timeout for OAM peers.

```
Router(config-if)# ethernet oam
```

- Step 6** Use the **exit** command to exit configuration mode.

```
Router(config)# exit
Router#
```

---

## Stopping and Starting Link Monitoring Operations

---

**Step 1** Enter enable mode.

```
Router> enable
```

**Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

**Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Step 4** Use the **interface** command to specify the interface you wish to configure.

```
Router(config)# interface gigabitethernet 0/3
Router(config-if)#
```

**Step 5** Use the **ethernet oam** command to enable Ethernet OAM on the interface. You can use the following parameters:

- **max-rate**—Sets the maximum rate per second for OAM PDUs.
- **min-rate**—Sets the minimum rate per second for OAM PDUs.
- **mode**—Sets the OAM client mode (active or passive).
- **timeout**—Specifies the timeout for OAM peers.

```
Router(config-if)# ethernet oam
```

**Step 6** Use the **ethernet oam link-monitor supported** command to enable link monitoring on the interface. You can use the **no** form of this command if you want to disable link monitoring.

```
Router(config-if)# ethernet oam link-monitor supported
```

**Step 7** Use the **exit** command to exit configuration mode.

```
Router(config)# exit
Router#
```

---

## Configuring Link Monitoring Options

---

**Step 1** Enter enable mode.

```
Router> enable
```

**Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.



- Step 3** Enter global configuration mode.
- ```
Router# configure terminal
```
- Enter configuration commands, one per line. End with CNTL/Z.
- Step 4** Use the **interface** command to specify the interface you wish to configure.
- ```
Router(config)# interface gigabitethernet 0/3
Router(config-if)#
```
- Step 5** Use the **ethernet oam** command to enable Ethernet OAM on the interface.
- ```
Router(config-if)# ethernet oam
```
- Step 6** Use the **ethernet oam link-monitor high-threshold** command to configure an error-disable function on the Ethernet OAM interface when a high threshold for an error is exceeded.
- ```
Router(config-if)# ethernet oam link-monitor high-threshold action error-disable-interface
```
- Step 7** Use the **ethernet oam link-monitor frame** command to configure a number for error frames that when reached triggers an action.
- ```
Router(config-if)# ethernet oam link-monitor frame window 399
```
- Step 8** Use the **ethernet oam link-monitor frame-period** command to configure a number of frames to be polled. Frame period is a user-defined parameter.
- ```
Router(config-if)# ethernet oam link-monitor frame-period threshold high 599
```
- Step 9** Use the **ethernet oam link-monitor frame-seconds** command to configure a period of time in which error frames are counted.
- ```
Router(config-if)# ethernet oam link-monitor frame-seconds window 699
```
- Step 10** Use the **ethernet oam link-monitor receive-crc** command to configure an Ethernet OAM interface to monitor ingress frames with cyclic redundancy check (CRC) errors for a period of time.
- ```
Router(config-if)# ethernet oam link-monitor receive-crc window 99
```
- Step 11** Use the **ethernet oam link-monitor transmit-crc** command to configure an Ethernet OAM interface to monitor egress frames with CRC errors for a period of time.
- ```
Router(config-if)# ethernet oam link-monitor transmit-crc threshold low 199
```
- Step 12** Use the **exit** command to exit configuration mode.
- ```
Router(config)# exit
Router#
```
- 

## Configuring Global Ethernet OAM Options Using a Template

Perform this task to create a template to use for configuring a common set of options on multiple Ethernet OAM interfaces. Steps 4 through 10 are optional and can be performed in any sequence. These steps may also be repeated to configure different options.

- 
- Step 1** Enter enable mode.
- ```
Router> enable
```

- Step 2** Enter the password.
- ```
Password: password
```
- When the prompt changes to `Router`, you have entered enable mode.
- Step 3** Enter global configuration mode.
- ```
Router# configure terminal
```
- Enter configuration commands, one per line. End with CNTL/Z.
- Step 4** Use the **template** command to configure a template and enter template configuration mode.
- ```
Router(config)# template oam-temp
```
- Step 5** Use the **ethernet oam link-monitor receive-crc** command to configure an Ethernet OAM interface to monitor ingress frames with cyclic redundancy check (CRC) errors for a period of time.
- ```
Router(config-if)# ethernet oam link-monitor receive-crc window 99
```
- Step 6** Use the **ethernet oam link-monitor transmit-crc** command to configure an Ethernet OAM interface to monitor egress frames with CRC errors for a period of time.
- ```
Router(config-if)# ethernet oam link-monitor transmit-crc threshold low 199
```
- Step 7** Use the **ethernet oam link-monitor symbol-period** command to configure a threshold or window for error symbols, in number of symbols.
- ```
Router(config-if)# ethernet oam link-monitor symbol-period threshold high 299
```
- Step 8** Use the **ethernet oam link-monitor high-threshold** command to configure an error-disable function on the Ethernet OAM interface when a high threshold for an error is exceeded.
- ```
Router(config-if)# ethernet oam link-monitor high-threshold action error-disable-interface
```
- Step 9** Use the **ethernet oam link-monitor frame** command to configure a number for error frames that when reached triggers an action.
- ```
Router(config-if)# ethernet oam link-monitor frame window 399
```
- Step 10** Use the **ethernet oam link-monitor frame-period** command to configure a number of frames to be polled. Frame period is a user-defined parameter.
- ```
Router(config-if)# ethernet oam link-monitor frame-period threshold high 599
```
- Step 11** Use the **ethernet oam link-monitor frame-seconds** command to configure a period of time in which error frames are counted.
- ```
Router(config-if)# ethernet oam link-monitor frame-seconds window 699
```
- Step 12** Use the **exit** command to exit configuration mode.
- ```
Router(config)# exit
Router#
```
- Step 13** Use the **interface** command to specify the interface to which you want to apply the template.
- ```
Router(config)# interface gigabitethernet 0/3
Router(config-if)#
```
- Step 14** Use the **source template** command to apply the configuration template to the interface.
- ```
Router(config-if)# source template oam-temp
```
- Step 15** Use the **end** command to exit configuration mode.

```
Router(config-if)# end
Router#
```

## Configuring a Port for RFI Support

**Step 1** Enter enable mode.

```
Router> enable
```

**Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

**Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Step 4** Use the **interface** command to specify the interface you wish to configure.

```
Router(config)# interface gigabitethernet 0/3
Router(config-if)#
```

**Step 5** Use the **ethernet oam remote-failure** command to configure failure messages critical event occurs. You can use set the following message types:

- critical-event
- dying-gasp
- link-fault



**Note**

Release 12.2(33)MRA does not support sending critical-event messages but can receive all three message types.

```
Router(config-if)# ethernet oam remote-failure dying-gasp action error-disable-interface
```

**Step 6** Use the **exit** command to exit configuration mode.

```
Router(config)# exit
Router#
```

## Configuring Ethernet Local Management Interface (E-LMI)

The following sections describe how to configure Ethernet LMI on the Cisco MWR 2941:

- [Enabling Ethernet LMI on All Supported Interfaces](#)
- [Enabling Ethernet LMI on a Single Supported Interface](#)

### Enabling Ethernet LMI on All Supported Interfaces

Follow these steps to enable Ethernet LMI on all supported interfaces on the Cisco MWR 2941.

- 
- Step 1** Enter enable mode.
- ```
Router> enable
```
- Step 2** Enter the password.
- ```
Password: password
```
- When the prompt changes to `Router`, you have entered enable mode.
- Step 3** Enter global configuration mode.
- ```
Router# configure terminal
```
- Enter configuration commands, one per line. End with CNTL/Z.
- Step 4** Use the **ethernet lmi global** command to enable Ethernet LMI on all interfaces.
- ```
Router(config)# ethernet lmi global
```
- Step 5** Use the **exit** command to exit configuration mode.
- ```
Router(config)# exit
Router#
```

### Enabling Ethernet LMI on a Single Supported Interface

Follow these steps to enable Ethernet LMI on a single supported interface on the Cisco MWR 2941.

- 
- Step 1** Enter enable mode.
- ```
Router> enable
```
- Step 2** Enter the password.
- ```
Password: password
```
- When the prompt changes to `Router`, you have entered enable mode.
- Step 3** Enter global configuration mode.
- ```
Router# configure terminal
```
- Enter configuration commands, one per line. End with CNTL/Z.
- Step 4** Use the **interface** command to specify the interface you wish to configure.

```
Router(config)# interface ethernet 1/3  
Router(config-if)#
```

**Step 5** Use the **ethernet lmi interface** command to enable Ethernet LMI on the interface.

```
Router(config)# ethernet lmi interface
```

**Step 6** Use the **exit** command to exit configuration mode.

```
Router(config)# exit  
Router#
```

## Configuring Clocking and Timing

The Cisco MWR 2941 supports the following network clocking types:

- Precision Time Protocol (PTP)—Clocking and clock recovery based on the IEEE 1588-2008 standard; allows the Cisco MWR 2941 router to receive clocking from another PTP-enabled device or provide clocking to a PTP-enabled device. To configure PTP clocking, see the [“Configuring PTP Clocking” section on page 4-39](#). If you want to enable PTP redundancy, see the [“Configuring IP Multicast” section on page 4-64](#).
- Pseudowire-based clocking—Allows the Cisco MWR 2941 router to use clocking using a pseudowire or virtual pseudowire interface. Pseudowire-based clocking supports adaptive clock recovery, which allows the Cisco MWR 2941 to recover clocking from the headers of a packet stream. To configure pseudowire-based clocking, see the [“Configuring Pseudowire-based Clocking with Adaptive Clock Recovery” section on page 4-45](#).
- Synchronous Ethernet—Allows the network to transport frequency and time information over Ethernet. To configure synchronous Ethernet, see the [“Configuring Synchronous Ethernet” section on page 4-47](#).
- Verifying Clock Settings—To verify a clocking configuration, see the [“Verifying Clock-related Settings” section on page 4-49](#).

**Note**

The Cisco MWR 2941 does not support the use of PTP and PWE-based clocking at the same time.

## Configuring PTP Clocking

This section describes how to configure PTP-based clocking on the Cisco MWR 2941. For more information about the PTP commands, see, [Appendix B, “Cisco MWR 2941 Router Command Reference.”](#)

**Note**

The settings shown in this section are an example only; you must determine the appropriate PTP settings based upon your network clocking design.

**Note**

The configuration sections describing the 1PPS and 10Mhz timing ports only apply to the Cisco MWR 2941-DC-A; the Cisco MWR-DC router does not have these timing ports.

## Configuring Global PTP Settings

**Step 1** Enter the following commands to configure the global PTP settings:

- a. Use the **ptp mode** command to specify the PTP mode.

```
Router(config)# ptp mode ordinary
```

- b. Use the **ptp priority1** command to configure the preference level for a clock; slave devices use the priority1 value when selecting a master clock.

```
Router(config)# ptp priority1 128
```

- c. Use the **ptp priority2** command to set a secondary preference level for a clock; slave devices use the priority2 value when selecting a master clock.

```
Router(config)# ptp priority2 128
```

- d. Use the **ptp domain** command to specify the PTP domain number that the router uses. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network.

```
Router(config)# ptp domain 6
```



**Note**

If you want to use PTP redundancy, see [Configuring IP Multicast, page 4-64](#).

## Configuring the PTP Mode

[Table 4-1](#) summarizes the PTP mode commands that you can use on the Cisco MWR 2941.



**Note**

If you want to use PTP redundancy, see [Configuring IP Multicast, page 4-64](#).

**Table 4-1 PTP Mode Commands**

| Command                | Purpose                                                                                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ptp announce           | Sets interval and timeout values for PTP announcement packets.                                                                                                         |
| ptp clock-destination  | Specifies the IP address of a clock destination. This command only applies when the router is in PTP master unicast mode.                                              |
| ptp clock-source       | Specifies the IP address of the clock source. This command only applies when the router is in PTP slave mode.                                                          |
| ptp delay-req interval | Specifies the delay request interval, the time recommended to member devices to send delay request messages when an interface is in PTP master mode.                   |
| ptp delay-req unicast  | Configures the Cisco MWR 2941 to send unicast PTP delay request messages while in multicast mode. This command helps reduce unnecessary PTP delay request traffic.     |
| ptp enable             | Enables PTP mode on an interface.                                                                                                                                      |
| ptp master             | Sets an interface in master clock mode for PTP clocking.<br><br><b>Note</b> PTP master mode is intended for trial use only and is not for use in a production network. |

Table 4-1 PTP Mode Commands

| Command   | Purpose                                                                           |
|-----------|-----------------------------------------------------------------------------------|
| ptp slave | Sets an interface to slave clock mode for PTP clocking.                           |
| ptp sync  | Specifies the interval that the router uses to send PTP synchronization messages. |

The following examples demonstrate how to use these commands to configure each of the PTP modes. Use the appropriate section based on the PTP mode that you want to configure on the Cisco MWR 2941.

- PTP multicast master mode—Sets the Cisco MWR 2941 to act as the master PTP clock. Multicast specifies that the router sends PTP messages to all the slaves listening on the PTP multicast group.

**Note**

PTP master mode is intended for trial use only and is not for use in a production network.

```
Router(config)# interface Vlan10
Router(config-if)# ip address 192.168.52.38 255.255.255.0
Router(config-if)# ip igmp join-group 224.0.1.129
Router(config-if)# ptp announce interval 0
Router(config-if)# ptp sync interval -6
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp master multicast
Router(config-if)# ptp enable
```

- PTP multicast slave mode—Sets the Cisco MWR 2941 to receive clocking from a PTP master device in multicast mode.

```
Router(config)# interface Vlan10
Router(config-if)# ip address 192.168.52.38 255.255.255.0
Router(config-if)# ip igmp join-group 224.0.1.129
Router(config-if)# ptp announce interval 0
Router(config-if)# ptp sync interval -6
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp slave multicast
Router(config-if)# ptp enable
```

- PTP multicast slave mode (with hybrid clocking)—Sets the Cisco MWR 2941 to receive phase from a PTP master device in multicast mode while using clock frequency obtained from the synchronous Ethernet port.

```
Router(config)# interface Vlan10
Router(config-if)# ip address 192.168.52.38 255.255.255.0
Router(config-if)# ip igmp join-group 224.0.1.129
Router(config-if)# ptp announce interval 0
Router(config-if)# ptp sync interval -6
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp slave multicast hybrid
Router(config-if)# ptp enable
```

**Note**

You can use the **ptp delay-req unicast** command to set the Cisco MWR 2941 to send unicast PTP Delay\_Req messages while in multicast mode in order to eliminate unnecessary multicast traffic. For more information about this command, see [Appendix B, “Cisco MWR 2941 Router Command Reference.”](#)

- PTP unicast master mode—Sets the Cisco MWR 2941 to act as the master PTP clock. Unicast specifies that the router sends PTP messages to a single slave host.

```
Router(config)# interface Vlan2
Router(config-if)# ip address 192.168.52.38 255.255.255.0
Router(config-if)# ptp announce interval 0
Router(config-if)# ptp sync interval -6
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp master unicast
Router(config-if)# ptp clock-destination 192.168.52.201
Router(config-if)# ptp enable
```

- PTP unicast master mode (with negotiation enabled)—Sets the Cisco MWR 2941 to send clocking to a single PTP slave device; the router allows the slave devices to negotiate their master clock device. When in the router is in PTP unicast master mode, you can specify up to 128 PTP clock destination devices.

**Note**

If you set the router to PTP master unicast mode with negotiation, you do not specify PTP clock destinations because the router negotiates to determine the IP addresses of the PTP slave devices.

**Note**

We recommend that you determine the number of destination devices to assign to a master clock based on traffic rates and available bandwidth.

```
Router(config)# interface Vlan2
Router(config-if)# ip address 192.168.52.38 255.255.255.0
Router(config-if)# ptp announce interval 0
Router(config-if)# ptp sync interval -6
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp master unicast negotiation
Router(config-if)# ptp enable
```

- PTP unicast slave mode—Sets the Cisco MWR 2941 to receive clocking from a single PTP master device.

```
Router(config)# interface Vlan2
Router(config-if)# ip address 192.168.52.38 255.255.255.0
Router(config-if)# ptp announce interval 3
Router(config-if)# ptp announce timeout 2
Router(config-if)# ptp sync interval -6
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp slave unicast
Router(config-if)# ptp clock-source 192.168.52.10
Router(config-if)# ptp enable
```

- PTP unicast slave mode (with negotiation enabled)—Sets the Cisco MWR 2941 to receive clocking from a PTP master devices; the router negotiates between up to 128 PTP master devices.

```
Router(config)# interface Vlan2
Router(config-if)# ip address 192.168.52.38 255.255.255.0
Router(config-if)# ptp announce interval 3
Router(config-if)# ptp announce timeout 2
Router(config-if)# ptp sync interval -6
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp slave unicast negotiation
Router(config-if)# ptp clock-source 192.168.52.10
Router(config-if)# ptp enable
```



**Note**

You can only configure one VLAN interface for PTP.

- PTP unicast slave mode (with hybrid clocking)—Sets the Cisco MWR 2941 to receive phase (ToD or 1PPS) from a single PTP master device while using clock frequency obtained from the synchronous Ethernet port.

```
Router(config)# interface Vlan2
Router(config-if)# ip address 192.168.52.38 255.255.255.0
Router(config-if)# ptp announce interval 3
Router(config-if)# ptp announce timeout 2
Router(config-if)# ptp sync interval -6
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp slave unicast negotiation hybrid
Router(config-if)# ptp clock-source 192.168.52.10
Router(config-if)# ptp enable
```

- PTP unicast slave mode (with hot standby master clock)—Sets the Cisco MWR 2941 to receive clocking from a single PTP master device and enables a standby master clock. When you enable a standby master clock, the Cisco MWR 2941 selects the best clock source between two PTP master clocks and switches dynamically between them if the clock quality of the standby clock is greater than that of the current master clock. If you define a standby master clock, both clock sources must be in the same VLAN. Setting a standby master clock in unicast mode is optional.

```
Router(config)# interface Vlan2
Router(config-if)# ip address 192.168.52.38 255.255.255.0
Router(config-if)# ptp announce interval 3
Router(config-if)# ptp announce timeout 2
Router(config-if)# ptp sync interval -6
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp slave unicast negotiation hybrid
Router(config-if)# ptp clock-source 192.168.52.10
Router(config-if)# ptp clock-source 192.168.52.150
Router(config-if)# ptp enable
```

## Configure the Global Network Clock

Use the **network-clock-select** command to configure clock selection for the entire network.

- If you configured the router for PTP master mode, set one or more external clock sources using the **network-clock-select** command with the synchronous ethernet, bits, E1, T1, or SHDSL interface parameters:

```
Router(config)# network-clock-select 1 BITS
Router(config)# network-clock-select 2 SYNC 0
Router(config)# network-clock-select 3 E1 0/0
Router(config)# network-clock-select 4 SHDSL 1/0.1
```

**Note**

For SHDSL connections, the subinterface number represents the wire that the Cisco MWR 2941 uses to receive clocking.

- If you configured the router for PTP slave mode, enter the following commands:

```
Router(config)# network-clock-select 1 PACKET-TIMING
Router(config)# network-clock-select hold-timeout 900
```

**Note**

The **network-clock-select hold-timeout** command is optional; the minimum recommended value in the slave mode is 900 seconds (15 minutes). For more information about this command, see [Appendix B, “Cisco MWR 2941 Router Command Reference.”](#)

## Configuring PTP Input and Output

The following section describes how to configure time of day messages, output clocking, and input clocking. You can use the 1pps and 10Mhz timing ports on the Cisco MWR 2941-DC-A to do the following:

- Provide or receive 1PPS time of day messages
- Provide output clocking at 10Mhz, 2.048Mhz, and 1.544Mhz
- Receive input clocking at 10Mhz, 2.048Mhz, and 1.544Mhz

**Note**

This section applies only to the Cisco MWR 2941-DC-A.

Follow these steps to configure PTP input and output:

- If you want to configure PTP input clocking using the 10Mhz timing port, complete the following steps:
  - Use the **ptp input** command to enable PTP input clocking at 10Mhz, 2.048Mhz, or 1.544Mhz.  

```
Router(config)# ptp input 10M
```
  - Use the **network-clock-select** command to select the port to use for input clocking.  

```
Router(config)# network-clock-select 10 10M
```

Input clocking applies when the router is in PTP master mode.

- To configure output clocking using the 10Mhz timing port, use the **ptp output** command to specify 10Mhz, 2.048Mhz, or 1.544Mhz output. Use this command when the router is in PTP slave mode.

```
Router(config)# ptp output 2.048M
```

- To configure the router to send time of day messages using the 1PPS port, use the **1pps** option with the **ptp input** or **ptp output** commands. Use the **pulse-width** parameter to specify the pulse width value. You can also use the **1pps rs422** to specify PTP input using the RS-422 port.

```
Router(config)# ptp input 1pps pulse-width 1000 ns
Router(config)# ptp output 1pps pulse-width 2000 ms
```

- To configure the time of day message format, use the **ptp tod** command.

```
Router(config)# ptp tod ubx delay 400
```

- To configure the router to periodically update the system calendar with PTP clock time, use the **ptp update-calendar** command.

```
Rouner(config)# ptp update-calendar
```

**Note**

To see configuration examples for input and output timing, see [PTP Sample Configurations, page A-38](#).

## Configuring Pseudowire-based Clocking with Adaptive Clock Recovery

The Cisco MWR 2941 supports the following adaptive clock recovery modes:

- In-band master mode—The Cisco MWR 2941 provides clocking to slave devices using the headers in a packet stream. To configure this clocking mode, see [Configuring In-Band Master Mode](#).
- In-band slave mode—The Cisco MWR 2941 receives clocking from a master clock using the headers from a packet stream. To configure this clocking mode, see [Configuring In-Band Slave Mode](#).
- Out-of-band slave mode—The Cisco MWR 2941 receives clocking from a master clock using dedicated packets for timing. To configure this clocking mode, see [Configuring Out-of-Band Slave Mode](#).



### Note

The Cisco MWR 2941 currently does not support out-of-band master mode.

### Configuring In-Band Master Mode

**Step 1** To configure in-band ACR master mode, you must configure Structure-agnostic TDM over Packet (SAToP) or Circuit Emulation Service (CES).

- The following example shows how to configure SAToP.

```
Router(config)# controller e1 0/0
Router(config-controller)# clock source internal
Router(config-controller)# cem-group 0 unframed
```

- The following example shows how to configure CES.

```
Router(config)# controller e1 0/0
Router(config-controller)# clock source internal
Router(config-controller)# cem-group 3 timeslots 1-31
```

**Step 2** Configure the loopback interface.

```
Router(config)# interface Loopback
Router(config-if)# ip address 10.88.88.99 255.255.255.255
```

**Step 3** Configure the VLAN interface.

```
Router(config)# interface Vlan1
Router(config-if)# ip address 192.168.52.2 255.255.255.0
Router(config-if)# no ptp enable
Router(config-if)# mpls ip
```

**Step 4** Configure MPLS.

```
Router(config)# mpls ldp router-id Loopback0 force
```

**Step 5** Configure the CEM interface.

```
Router(config)# interface cem 0/1
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.2 7600 encaps mpls
```

**Step 6** Set one or more external clock sources using the synce, bits, E1, or T1 interface parameters:

```
Router(config)# network-clock-select 1 BITS
```

## Configuring In-Band Slave Mode

**Step 1** To configure in-band ACR slave mode, you must configure Structure-agnostic TDM over Packet (SAToP) or Circuit Emulation Service (CES).

- The following example shows how to configure SAToP.

```
Router(config)# controller e1 0/0
Router(config-controller)# clock source internal
Router(config-controller)# cem-group 0 unframed
```

- The following example shows how to configure CES.

```
Router(config)# controller e1 0/0
Router(config-controller)# clock source internal
Router(config-controller)# cem-group 3 timeslots 1-31
```

**Step 2** Enter the following commands to configure the loopback interface.

```
Router(config)# interface Loopback
Router(config-if)# ip address 10.88.88.99 255.255.255.255
```

**Step 3** Enter the following commands to configure the VLAN interface.

```
Router(config)# interface Vlan1
Router(config-if)# ip address 192.168.52.10.2 255.255.255.0
Router(config-if)# no ptp enable
Router(config-if)# mpls ip
```

**Step 4** Enter the following command to configure MPLS.

```
Router(config)# mpls ldp router-id Loopback0 force
```

**Step 5** Enter the following commands to configure the CEM interface.

```
Router(config)# interface cem 0/0
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.2 7600 encaps mpls
```

**Step 6** Enter the following command to configure adaptive clock recovery using a circuit emulation (CEM) interface:

```
Router(config)# recovered-clock recovered adaptive cem 0 0 0
```

**Step 7** Enter the following commands to configure the network clock:

```
Router(config)# network-clock-select 1 PACKET-TIMING
Router(config)# network-clock-select hold-timeout 900
```

## Configuring Out-of-Band Slave Mode



### Note

When configuring out-of-band clocking, verify that the edge router (such as the Cisco 7600 Series Router) has matching settings for out-of-band clocking.

**Step 1** Enter the following command to configure clock recovery in slave mode:

```
Router(config)# recovered-clock slave
```

**Step 2** Enter the following commands to configure the loopback interface.

```
Router(config)# interface Loopback
```

```
Router(config-if)# ip address 10.88.88.99 255.255.255.255
```

**Step 3** Enter the following commands to configure the VLAN interface.

```
Router(config)# interface Vlan1
Router(config-if)# ip address 192.168.52.10.2 255.255.255.0
Router(config-if)# no ptp enable
Router(config-if)# mpls ip
```

**Step 4** Enter the following command to configure MPLS.

**Step 5** Router(config)# **mpls ldp router-id Loopback0 force**

**Step 6** Enter the following commands to configure the CEM interface.

```
Router(config)# interface virtual-cem 0/24
Router(config-if)# payload-size 486
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.2 7600 encaps mpls
```



**Note**

The Cisco MWR 2941 only supports a payload size of 486 (625 packets per second) or 243 (1250 packets per second). This value affects the payload size only and does not alter the packet size, which is constant regardless of payload value.

**Step 7** Enter the following commands to configure the network clock:

```
Router(config)# network-clock-select 1 PACKET-TIMING
Router(config)# network-clock-select hold-timeout 900
```

## Configuring Synchronous Ethernet

The following sections describe how to configure synchronous Ethernet timing on the Cisco MWR 2941.

### Configuring an External Clock Source

To configure an external clock source using synchronous Ethernet, use the **network-clock select** command.

```
Router(config)# network-clock-select 2 SYNC 0
```

## Configuring Network Clock Quality Selection Using REP

Network clock quality selection with REP uses the Ethernet Synchronization Message Channel (ESMC) to indicate the quality of a clock source on a REP network segment. Network clock quality selection with REP also requires that you configure the following features:

- Holdoff timer—Defines the amount of time router waits before taking action when a synchronous Ethernet clock source fails. After the holdoff timer expires, the router announces the failure and takes one of the following actions depending on the clocking configuration:
  - Considers other clock sources.
  - Switches to holdover mode. The router generates a timing signal based on the stored timing reference.

The holdoff timer is a global timer value; it applies to both synchronous Ethernet clock sources when configured.

- **Restore timer**—Specifies the amount of time that the router waits before considering a synchronous clock source when the clock source becomes available. A restore timer helps maintain a stable clock source in the event that connectivity to a clock source is interrupted. The restore timer is a global timer value; it applies to both synchronous Ethernet clock sources when configured.

**Note**

The holdoff and restore timers described in this section are specific to Network clock quality selection with REP; they do not apply to other features on the Cisco MWR 2941.

For more information about network clock quality selection with REP, see [Network Clock Quality Selection using REP, page 1-17](#). For more information about REP, see [Resilient Ethernet Protocol \(REP\), page 1-5](#).

**Note**

You must configure REP before configuring ESMC. For instructions on how to configure REP, see [Configuring Resilient Ethernet Protocol \(REP\), page 4-15](#).

Follow these steps to configure network clock quality selection on the Cisco MWR 2941.

**Step 1** Enter enable mode.

```
Router> enable
```

**Step 2** Enter the password.

```
Password: password
```

When the prompt changes to *Router*, you have entered enable mode.

**Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Step 4** Use the **ql-enabled rep-segment** command to specify the REP segment that is configured for network clock quality selection. This command requires that you specify a synchronous Ethernet clock source.

```
Router(config)# ql-enabled rep-segment 10
```

**Step 5** Use the **network-clock-select hold-off-timeout** command to specify the value of the holdoff timer. Valid values are 0 or 50-10000 ms.

```
Router(config)# network-clock-select hold-off-timeout 1000
```

**Step 6** Use the **network-clock-select wait-to-restore** command to specify the value of the restore timer in seconds. Valid values are 0–720 seconds or up to 12 minutes.

```
Router(config)# network-clock-select wait-to-restore 360
```

**Step 7** Exit configuration mode.

```
Router(config)# exit
Router#
```

You can use the **show network-clocks** command to verify your configuration.

## Verifying Clock-related Settings

Use the following commands to verify the clock settings

- [show network-clocks](#)—Displays information about the network clocks
- [show controller](#)—Displays the status of the controller, including clocking information.
- [show ptp clock](#)—Displays ptp clock information
- [show ptp foreign-master-record](#)—Displays PTP foreign master records
- [show ptp parent](#)—Displays PTP parent properties
- [show ptp port](#)—Displays PTP port properties
- [show ptp time-property](#)—Displays PTP clock time properties
- [show cem circuit](#)—Displays information about the CEM circuit
- [show platform hardware](#)—Displays the status of hardware devices on the Cisco MWR 2941.
- [show platform hardware rtm](#)—Displays the current status of the TOP module

## Configuring MLPPP Backhaul

To configure an MLPPP backhaul, complete the following tasks:

- [Configuring the Card Type, page 4-49](#)
- [Configuring E1 Controllers, page 4-50](#)
- [Configuring T1 Controllers, page 4-52](#)
- [Configuring a Multilink Backhaul Interface, page 4-54](#)

## Configuring the Card Type

Perform a basic card type configuration by enabling the router, enabling an interface, and specifying the card type as described below. You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.



### Note

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

To select and configure a card type, follow these steps:

**Step 1** Enter enable mode.

```
Router> enable
```

**Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

**Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

When the prompt changes to `Router(config)`, you have entered global configuration mode.



**Note** To view a list of the configuration commands available to you, enter `?` at the prompt or press the **Help** key while in configuration mode.

**Step 4** Set the card type.

Router(config-if)# **card type** {**e1** | **t1**} *slot subslot*

- *slot*—Slot number of the interface.
- *subslot*—Specifies the VWIC slot number.

For example, the following command shows how to configure a T1/E HWIC in the first HWIC slot as an E1 card:

Router(config)# **card type e1 0 1**

When the command is used for the first time, the configuration takes effect immediately. A subsequent change in the card type does not take effect unless you enter the **reload** command or reboot the router.



**Note** When you are using the **card type** command to change the configuration of an installed card, you must first enter the **no card type** {**e1** | **t1**} *slot subslot* command. Then enter the **card type** {**e1** | **t1**} *slot subslot* command for the new configuration information.

## Configuring E1 Controllers

Perform a basic E1 controller configuration by specifying the E1 controller, entering the clock source, specifying the channel-group, configuring the serial interface, configuring PPP encapsulation, and enabling keepalive packets. You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.



**Note** In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

To configure the E1 controllers, follow these steps while in global configuration mode:

**Step 1** Specify the controller that you want to configure. Controller E1 0/0 maps to the T1/E1 HWIC card in HWIC slot 0.

Router(config)# **controller e1** *slot/port*

For example, the following command shows how to specify the E1 controller as the first port of the T1/E1 HWIC card in slot 0:

Router(config)# **controller e1 0/0**  
Router(config-controller)#



The prompt changes to `Router(config-controller)`, when you enter controller configuration mode.

**Step 2** Specify the framing type.

```
Router(config-controller)# framing {crc4 | no-crc4}
```

**Step 3** Specify the line code format.

```
Router(config-controller)# linecode {ami | hdb3}
```

**Step 4** Use the **mode** command to set the controller in asynchronous transfer mode (ATM) or channel-associated signaling (CAS) mode.

```
Router(config-controller)# mode {atm | cas}
```

**Step 5** Enter the clocking source.

```
Router(config-controller)# clock source {line | internal} [bits]
```

- *line*—Specifies the E1 line from which the clocking is taken.
- *internal*—Specifies internal clocking.
- *bits*—Enabled Building Integrated Timing Supply (BITS) clocking.

For example, the following command shows how to configure the clock source for the E1 controller:

```
Router(config-controller)# clock source line
```



**Note** When you are using the **clock source** command to change the configuration of an installed card, you must enter the **no clock source** command first. Then, enter the **clock source** command for the new configuration information.

**Step 6** Specify the channel-group and time slots to be mapped. After you configure a channel-group, the serial interface is automatically created.

```
Router(config-controller)# channel-group channel-no timeslots timeslot-list speed {64}
```

- *channel-no*—ID number to identify the channel group. The valid range is 0 to 30.
- *timeslot-list*—Timeslots (DS0s) to include in this channel group. The valid timeslots are 1 to 31.
- **speed {64}**—The speed of the DS0: 64 kbps.

For example, the following command configures the channel-group and time slots for the E1 controller:

```
Router(config-controller)# channel-group 0 timeslots 1-31 speed 64
```



**Note** When you are using the **channel-group channel-no timeslots timeslot-list {64}** command to change the configuration of an installed card, you must enter the **no channel-group channel-no timeslots timeslot-list speed {64}** command first. Then, enter the **channel-group channel-no timeslots timeslot-list {64}** command for the new configuration information.

**Step 7** Exit controller configuration mode.

```
Router(config-controller)# exit
```

**Step 8** Configure the serial interface. Specify the E1 slot, port number, and channel-group.

```
Router(config)# interface serial slot/port:channel
```

When the prompt changes to `Router(config-if)`, you have entered interface configuration mode.

**Note**

To see a list of the configuration commands available to you, enter **?** at the prompt or press the **Help** key while in the configuration mode.

- Step 9** To configure PPP encapsulation, enter the following command:

```
Router(config-if)# encapsulation ppp
```

- Step 10** Enable keepalive packets on the interface and specify the number of times keepalive packets are sent without a response before bringing down the interface:

```
Router(config-if)# keepalive [period [retries]]
```

- Step 11** Exit interface configuration mode.

```
Router(config-if)# exit
```

## Configuring T1 Controllers

Use the following instructions to perform a basic T1 controller configuration: specifying the T1 controller, specifying the framing type, specifying the line code form, specifying the channel-group and time slots to be mapped, configuring the cable length, configuring the serial interface, configuring PPP encapsulation, and enabling keepalive packets. You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.

**Note**

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the **Router#** prompt.

To configure the T1 interfaces, follow these steps while in the global configuration mode:

- Step 1** Specify the controller that you want to configure. Controller T1 0/0 maps to the T1/E1 HWIC card in HWIC slot 0.

```
Router(config)# controller t1 slot/port
```

- Step 2** Specify the framing type.

```
Router(config-controller)# framing esf
```

- Step 3** Specify the line code format.

```
Router(config-controller)# linecode b8zs
```

- Step 4** Use the **mode** command to set the controller in asynchronous transfer mode (ATM) or channel-associated signaling (CAS) mode.

```
Router(config-controller)# mode {atm | cas}
```

- Step 5** Specify the channel-group and time slots to be mapped. After you configure a channel-group, the serial interface is automatically created.

**Note**

The default speed of the channel-group is 56.

```
Router(config-controller)# channel-group 0 timeslots 1-24 speed 56
```

- Step 6** Configure the cable length.

```
Router(config-controller)# cablelength {long [-15db | -22.5db | -7.5db | 0db] short [110ft  
| 220ft | 330ft | 440ft | 550ft | 600ft]}
```

- Step 7** Exit controller configuration mode.

```
Router(config-controller)# exit
```

- Step 8** Configure the serial interface. Specify the T1 slot (always 0), port number, and channel-group.

```
Router(config)# interface serial slot/port:channel
```

- Step 9** Enter the following command to configure PPP encapsulation.

```
Router(config-if)# encapsulation ppp
```

- Step 10** Enable keepalive packets on the interface and specify the number of times that keepalive packets will be sent without a response the interface is brought down:

```
Router(config-if)# keepalive [period [retries]]
```

- Step 11** Exit to global configuration mode.

```
Router(config-if)# exit
```

## Configuring ATM IMA

Inverse multiplexing provides the capability to transmit and receive a single high-speed data stream over multiple slower-speed physical links. In inverse multiplexing over ATM (IMA), the originating stream of ATM cells is divided so that complete ATM cells are transmitted in round-robin order across the set of ATM links. Follow these steps to configure ATM IMA on the Cisco MWR 2941.

- Step 1** Use the **card type** command to specify the slot and port number of the E1 or T1 interface.

```
Router(config)# card type e1 0 0
```

- Step 2** Specify the controller interface on which you want to enable IMA.

```
Router(config)# controller E1 0/4  
Router(config-controller)#
```

- Step 3** Set the clock source to internal.

```
Router(config-controller)# clock source internal
```

- Step 4** Use the **ima-group** command to assign the interface to an IMA group, and set the scrambling-payload parameter to randomize the ATM cell payload frames. This command assigns the interface to IMA group 0.

```
Router(config-controller)# ima-group 0 scrambling-payload
```



**Note** This command automatically creates an ATM0/IMAx interface.

- Step 5** To add another member link, repeat [Step 1](#) to [Step 4](#).

- Step 6** Type **exit** to exit the controller interface.

```
Router(config-controller)# exit  
Router(config)#
```

**Step 7** Specify the slot location and port of IMA interface group.

```
Router(config-if)# interface ATM slot/IMA group-number
```

- *slot*—Specifies the slot location of the ATM IMA port adapter.
- *group-number*—Specifies the group number of the IMA group.

For example, the following command specifies the slot number as 0 and the group number as 0:

```
Router(config-if)# interface atm0/ima0
```



**Note** To explicitly configure the IMA group ID for the IMA interface, you may use the optional **ima group-id** command. You cannot configure the same IMA group ID on two different IMA interfaces; therefore, if you configure an IMA group ID with the system-selected default ID already configured on an IMA interface, the system toggles the IMA interface to make the user-configured IMA group ID the effective IMA group ID. At the same, the system toggles the original IMA interface to select a different IMA group ID.

**Step 8** Disable the IP address configuration for the physical layer interface.

```
Router(config-if)# no ip address
```

**Step 9** Specify the ATM bandwidth as dynamic.

```
Router(config-if)# atm bandwidth dynamic
```

**Step 10** Disable the Interim Local Management Interface (ILMI) keepalive parameters.

```
Router(config-if)# no atm ilmi-keepalive
```



**Note** The above configuration has one IMA shorthaul with two member links (atm0/0 and atm0/1).

## Configuring a Multilink Backhaul Interface

A multilink interface is a virtual interface that represents a multilink PPP bundle. The multilink interface coordinates the configuration of the bundled link, and presents a single object for the aggregate links. However, the individual PPP links that are aggregated must also be configured. Therefore, to enable multilink PPP on multiple serial interfaces, you first need to set up the multilink interface, and then configure each of the serial interfaces and add them to the same multilink interface.



**Note** In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

The Cisco MWR 2941 router can support up to 16 E1/T1 connections through the multilink interface, ranging from 12 bundles of 1 E1/T1 each to a single bundle containing 16 E1/T1 bundles.

Complete the following tasks to configure a multilink backhaul interface:

- [Creating a Multilink Bundle, page 4-55](#)
- [Configuring PFC and ACFC, page 4-55](#)
- [Enabling Multilink and Identifying the Multilink Interface, page 4-57](#)
- [For more information about configuring MLPPP, see the Cisco IOS Dial Technologies Configuration Guide, Release 12.2SR., page 4-58](#)

## Creating a Multilink Bundle

To create a multilink bundle, follow these steps while in the global configuration mode:

**Step 1** Create a multilink bundle and enter the interface configuration mode:

```
Router(config)# interface multilink group-number
```

- *group-number*—Number of the multilink bundle.

For example, the following command creates a multilink bundle 5:

```
Router(config)# interface multilink5  
Router(config-if)#
```

To remove a multilink bundle, use the **no** form of this command.



**Note** To see a list of the configuration commands available to you, enter **?** at the prompt or press the **Help** key while in the configuration mode.

**Step 2** Assign an IP address to the multilink interface.

```
Router(config-if)# ip address address [subnet mask]
```

- *address*—The IP address.
- *subnet mask*—Network mask of IP address.

For example, the following command creates an IP address and subnet mask:

```
Router(config-if)# ip address 10.10.10.2 255.255.255.0
```

## Configuring PFC and ACFC

Protocol-Field-Compression (PFC) and Address-and-Control-Field-Compression (ACFC) are PPP compression methods defined in RFCs 1661 and 1662. PFC allows for compression of the PPP Protocol field; ACFC allows for compression of the PPP Data Link Layer Address and Control fields.

Use the following instructions to perform PFC and ACFC handling during PPP negotiation to be configured. By default, PFC/ACFC handling is not enabled.



**Note** The recommended PFC and ACFC handling in the Cisco MWR 2941 router is: **acfc local request, acfc remote apply, pfc local request, and pfc remote apply**.

### Configuring PFC

To configure PFC handling during PPP negotiation, follow these steps, while in the interface configuration mode:

- Step 1** To configure how the router handles PFC in its outbound configuration requests, enter the following command:

```
Router(config-if)# ppp pfc local {request | forbid}
```

Where:

- **request**—The PFC option is included in outbound configuration requests.
- **forbid**—The PFC option is not sent in outbound configuration requests, and requests from a remote peer to add the PFC option are not accepted.

For example, the following command shows how to create a method for the router to manage PFC:

```
Router(config-if)# ppp pfc local request
```

- Step 2** To configure a method for the router to use to manage the PFC option in configuration requests received from a remote peer, enter the following command:

```
Router(config-if)# ppp pfc remote {apply | reject | ignore}
```

Where:

- **apply**—PFC options are accepted and ACFC may be performed on frames sent to the remote peer.
- **reject**—PFC options are explicitly ignored.
- **ignore**—PFC options are accepted, but ACFC is not performed on frames sent to the remote peer.

For example, issuing the following command allows PFC options to be accepted:

```
Router(config)# ppp pfc remote apply
```

### Configuring ACFC

To configure ACFC handling during PPP negotiation, follow these steps, while in interface configuration mode:

- Step 1** To configure how the router handles ACFC in its outbound configuration requests, enter the following command:

```
Router(config-if)# ppp acfc local {request | forbid}
```

Where:

- **request**—The ACFC option is included in outbound configuration requests.
- **forbid**—The ACFC option is not sent in outbound configuration requests, and requests from a remote peer to add the ACFC option are not accepted.

For example, the following command creates how the router handles ACFC:

```
Router(config-if)# ppp acfc local request
```

- Step 2** To configure how the router handles the ACFC option in configuration requests received from a remote peer, enter the following command:

```
Router(config-if)# ppp acfc remote {apply | reject | ignore}
```

Where:

- **apply**—ACFC options are accepted and ACFC may be performed on frames sent to the remote peer.
- **reject**—ACFC options are explicitly ignored.
- **ignore**—ACFC options are accepted, but ACFC is not performed on frames sent to the remote peer.

For example, the following command allows ACFC options to be accepted:

```
Router(config-if)# ppp acfc remote apply
```

## Enabling Multilink and Identifying the Multilink Interface

To enable multilink and identify the multilink interface, follow these steps, while in interface configuration mode:



### Note

If you modify parameters for an MLPPP bundle while it is active, the changes do not take effect until the Cisco MWR 2941 renegotiates the bundle connection.

#### Step 1 Enable multilink PPP operation.

```
Router(config-if)# ppp multilink
```

#### Step 2 Specify an identification number for the multilink interface.

```
Router(config-if)# ppp multilink group group-number
```

- ***group-number***—Multilink group number.

For example, the following command restricts (identifies) the multilink interface, 5, that can be negotiated:

```
Router(config-if)# ppp multilink group 5
```

#### Step 3 Enable keepalive packets on the interface and specify the number of times the keepalive packets are sent without a response before bringing down the interface.

```
Router(config-if)# keepalive [period [retries]]
```

- ***period***—(Optional) Integer value in seconds greater than 0. The default is 10.
- ***retries***—(Optional) Specifies the number of times that the device will continue to send keepalive packets without response before bringing the interface down. Integer value greater than 1 and less than 255. If omitted, the value that was previously set is used; if no value was specified previously, the default of 5 is used.

For example, the following command shows how to restrict (identify) the multilink interface, 5, that can be negotiated:

```
Router(config-if)# keepalive 1 5
```

### MLPPP Offload

By default, the Cisco MWR 2941 offloads processing for distributed MLPPP (dMLPPP) to the network processor for improved performance. However, the Cisco MWR 2941 does not support some dMLPPP settings on offloaded bundles. The Cisco MWR 2941 does not support the following options on offloaded dMLPPP bundles:

- **ppp multilink idle-link**
- **ppp multilink queue depth**
- **ppp multilink fragment maximum**
- **ppp multilink slippage**
- **ppp timeout multilink lost-fragment**

**Note**

---

If you have a bundle that requires the use of these options, contact Cisco support for assistance.

---

For more information about MLPPP offload, see the [“MLPPP Optimization Features” section on page 1-32](#).

---

## Configuring Additional MLPPP Settings

You can perform a variety of other configurations on an MLPPP bundle, including the following:

- Modifying the maximum fragment size
- Modifying fragmentation settings
- Enabling or disabling fragmentation
- Enabling or disabling interleaving
- Configuring distributed MLPPP (dMLPPP)
- Configuring multiclass MLPPP

For more information about configuring MLPPP, see the [Cisco IOS Dial Technologies Configuration Guide, Release 12.2SR](#).

## Configuring Multiprotocol Label Switching (MPLS)

Several technologies such as pseudowires utilize MPLS for packet transport. For more information about how to configure MPLS, see the [Cisco IOS Multiprotocol Label Switching Configuration Guide, Release 12.2SR](#).

**Note**

---

The Cisco MWR 2941 does not necessarily support all of the commands listed in the Release 12.2SR documentation.

---



## Configuring Routing Protocols

The Cisco MWR 2941 supports the following routing protocols:

- OSPF—An Interior Gateway Protocol (IGP) designed expressly for IP networks that supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets.
- IS-IS—An Open System Interconnection (OSI) protocol that specifies how routers communicate with routers in different domains.
- BGP—An interdomain routing protocol designed to provide loop-free routing between separate routing domains that contain independent routing policies (autonomous systems).

For instructions on how to configure OSPF, IS-IS, and BGP, see the [Cisco IOS IP Routing Protocols Configuration Guide, Release 12.2SR](#).

**Note**

The Cisco MWR 2941 does not support the other routing protocols listed in this document.

## Configuring BFD

Bidirectional Forwarding Detection (BFD) provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent routers, including the interfaces, data links, and forwarding planes. BFD is a detection protocol that you enable at the interface and routing protocol levels. Cisco supports the BFD asynchronous mode, in which two routers exchange BFD control packets to activate and maintain BFD neighbor sessions. To create a BFD session, you must configure BFD on both systems (or BFD peers). Once you have enabled BFD on the interface and the router level for the appropriate routing protocols, a BFD session is created, BFD timers are negotiated, and the BFD peers begin to send BFD control packets to each other at the negotiated interval.

The following sections describe how to configure BFD for each routing protocol.

- [Configuring BFD for OSPF](#)
- [Configuring BFD for BGP](#)
- [Configuring BFD for IS-IS](#)
- [Configuring BFD for Static Routes](#)

For more information about BFD, refer to the [Cisco IOS IP Routing Protocols Configuration Guide, Release 12.2SR](#). For a sample BFD configurations, see [Appendix A, “Sample Configurations.”](#)

### Configuring BFD for OSPF

This section describes how to configure BFD on the Cisco MWR 2941.

#### Configuring BFD for OSPF on One or More Interfaces

Follow these steps to configure BFD for OSPF on a single interface.

**Step 1** Enter enable mode.

```
Router> enable
```

**Step 2** Enter the password.

Password: *password*

When the prompt changes to *Router*, you have entered enable mode.

- Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

- Step 4** Use the **interface** command to specify the interface you wish to configure.

```
Router(config)# interface vlan1  
Router(config-if)#
```

- Step 5** Use the **ip ospf bfd** command to enable BFD for OSPF.

```
Router(config-if)# ip ospf bfd
```

- Step 6** Use the **bfd interval** command to specify the BFD session parameters.

```
Router(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

- Step 7** Enter the **end** command to exit configuration mode

```
Router(config)# end  
Router#
```



**Note**

You can also use the **show bfd neighbors** and **show ip ospf** commands to display troubleshooting information about BFD and OSPF.

## Configuring BFD for OSPF on All Interfaces

- Step 1** Enter enable mode.

```
Router> enable
```

- Step 2** Enter the password.

Password: *password*

When the prompt changes to *Router*, you have entered enable mode.

- Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

- Step 4** Use the **router ospf process-id** command to create a configuration for an OSPF process.

```
Router(config)# router ospf 100
```

- Step 5** Use the **bfd all-interfaces** command to enable BFD globally on all interfaces associated with the OSPF routing process.

```
Router(config)# bfd all-interfaces
```

- Step 6** Enter the end command to exit configuration mode

```
Router(config)# end
```

Router#

**Note**

You can disable BFD on a single interface using the **ip ospf bfd disable** command when configuring the relevant interface.

## Configuring BFD for BGP

Follow these steps to configure BFD for BGP.

- 
- Step 1** Enter enable mode.
- ```
Router> enable
```
- Step 2** Enter the password.
- ```
Password: password
```
- When the prompt changes to Router, you have entered enable mode.
- Step 3** Enter global configuration mode.
- ```
Router# configure terminal
```
- Enter configuration commands, one per line. End with CNTL/Z.
- Step 4** Use the **router bgp** command to specify a BGP process and enter router configuration mode.
- ```
Router(config)# router bgp as-tag
```
- Step 5** Use the **neighbor** command to enable support for BFD failover.
- ```
Router(config)# neighbor ip-address fall-over bfd
```
- Step 6** Enter the **end** command to exit configuration mode
- ```
Router(config)# end
Router#
```
- Step 7** You can use the following commands to verify the BFD configuration.
- **show bfd neighbors [details]** —Verifies that the BFD neighbor is active and displays the routing protocols that BFD has registered.
  - **show ip bgp neighbor**—Displays information about BGP and TCP connections to neighbors.

## Configuring BFD for IS-IS

This section describes how to configure BFD for IS-IS routing.

### Configuring BFD for IS-IS on a Single Interface

Follow these steps to configure BFD for IS-IS on a single interface.

- 
- Step 1** Enter enable mode.
- ```
Router> enable
```

- Step 2** Enter the password.

Password: *password*

When the prompt changes to *Router*, you have entered enable mode.

- Step 3** Enter global configuration mode.

Router# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

- Step 4** Use the **interface** command to enter interface configuration mode.

Router(config)# **interface** *vlan1*

Router(config-if)#

- Step 5** Use the **ip router isis** command to enable support for IPv4 routing on the interface.

Router(config-if) **ip router isis** [*tag*]

- Step 6** Use the **isis bfd** command to enable BFD on the interface.

Router(config-if)# **isis bfd**



**Note**

You can use the **show bfd neighbors** and **show clns interface** commands to verify your configuration.

## Configuring BFD for IS-IS for All Interfaces

- Step 1** Enter enable mode.

Router> **enable**

- Step 2** Enter the password.

Password: *password*

When the prompt changes to *Router*, you have entered enable mode.

- Step 3** Enter global configuration mode.

Router# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

- Step 4** Use the **router isis** command to specify an IS-IS process and enter router configuration mode.

Router(config)# **router isis** [*area-tag*]

Router(config-router)#

- Step 5** Use the **bfd all-interfaces** command to enable BFD globally on all interfaces associated with the IS-IS routing process.

Router(config-router)# **bfd all-interfaces**

- Step 6** Enter the **exit** command to exit the interface.

Router(config-router)# **exit**

Router(config)#

**Step 7** If you want to enable BFD on a per-interface basis for one or more interfaces associated with the IS-IS routing process, complete the following steps:

- a. Use the **interface** command to enter interface configuration mode.

```
Router(config)# interface vlan1
Router(config-if)#
```

- b. Use the **ip router isis** command to enable support for IPv4 routing on the interface.

```
Router(config-if) ip router isis [tag]
```

- c. Use the **isis bfd** command to enable BFD on the interface.

```
Router(config-if)# isis bfd
```

**Step 8** Enter the end command to exit configuration mode

```
Router(config-if)# end
Router#
```

**Note**

You can use the **show bfd neighbors** and **show clns interface** commands to verify your configuration.

## Configuring BFD for Static Routes

Follow these steps to configure BFD for static routes.

**Step 1** Enter enable mode.

```
Router> enable
```

**Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

**Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Step 4** Use the **interface** command to specify an interface and enter interface configuration mode.

```
Router(config)# interface vlan1
```

**Step 5** Configure an IP address for the interface.

```
Router(config-if)# ip address 10.201.201.1 255.255.255.0
```

**Step 6** Enable BFD on the interface.

```
Router(config-if)# bfd interval 500 min_rx 500 multiplier 5
```

**Step 7** Exit interface configuration mode.

```
Router(config-if)# exit
Router(config)#
```

**Step 8** Specify a static route BFD neighbor.

```
Router(config)# ip route static bfd vlan1 10.201.201.2
```

```
Router(config)# ip route 10.0.0.0 255.0.0.0 vlan1 10.201.201.2
```

**Step 9** Exit configuration mode

```
Router(config)# end
Router#
```

You can use the **show ip static route** command to verify your configuration.

---

## Configuring IP Multicast

The Cisco MWR 2941 supports two modes of multicast:

- [Configuring Multicast in Sparse Mode with a Static Rendezvous Point](#)—A rendezvous point (RP) is required in networks running Protocol Independent Multicast sparse mode (PIM-SM). In PIM-SM, traffic is forwarded only to network segments with active receivers that have explicitly requested multicast data.
- [Configuring Source-Specific Multicast](#)—Source Specific Multicast (SSM). SSM is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (not shared trees) are created.

The Cisco MWR 2941 also supports the following Multicast features.

- [Source Specific Multicast \(SSM\) Mapping](#)—SSM Mapping extends the Cisco IOS suite of SSM transition tools, which also includes URL Rendezvous Directory (URD) and Internet Group Management Protocol Version 3 Lite (IGMP v3lite). SSM mapping supports SSM transition in cases where neither URD nor IGMP v3lite is available, or when supporting SSM on the end system is impossible or unwanted due to administrative or technical reasons. For instructions on how to configure SSM Mapping, see [Configuring Source Specific Multicast Mapping](#).
- [Multicast VPN](#)—The Cisco MWR 2941 also supports Multicast VPN (MVPN) feature. MVPN provides the ability to support multicast over a Layer 3 Virtual Private Network (VPN). For instructions on how to configure MVPN, see [Configuring Multicast VPN](#).

To verify your IP Multicast configuration, see [Verifying a Multicast Configuration](#).

For more information about configuring Multicast, see the [Cisco IOS IP Multicast Configuration Guide, Release 12.2SR](#).



**Note**

The Cisco MWR 2941 does not support all of the commands described in the Cisco IOS Release 12.2SR documentation.

---

## Configuring Multicast in Sparse Mode with a Static Rendezvous Point

A rendezvous point (RP) is required in networks running Protocol Independent Multicast sparse mode (PIM-SM). In PIM-SM, traffic will be forwarded only to network segments with active receivers that have explicitly requested multicast data.

Follow these steps to configure multicast in sparse mode with a static RP.

---

**Step 1** Enter enable mode.

```
Router> enable
```

**Step 2** Enter configuration mode.

```
Router# configure terminal
```

**Step 3** Complete the following steps to create an access list to permit specific Multicast Groups for use with the static RP configuration.

- a. Use the **ip access-list** command to define a standard IP access list.

```
Router(config)# ip access-list standard SSM
```

- b. Use the **permit** command to allow traffic from multicast groups. Repeat this step for each network from which you want to allow traffic.

```
Router(config)# access-list 2 permit 239.193.0.0 0.0.255.255
```

```
Router(config)# access-list 2 permit 239.194.0.0 0.0.255.255
```



**Note**

Access lists are required for sparse mode with a single static RP; ensure that you configure ACLs before completing the Multicast configuration. For more information about using access control lists (ACLs), see [Creating an IP Access List and Applying It to an Interface](#).

**Step 4** Use the **ip multicast-routing** command to enable IP multicast routing. You can use the **distributed** keyword to enable Multicast Distributed Switching.

```
Router(config)# ip multicast-routing
```

**Step 5** By default, the IP address of the outgoing interface of the designated router (DR) leading toward the RP is used as the IP source address of a register message. If you want to configure another IP source address, use the **ip pim register-source** command to specify another interface.

```
Router(config)# ip pim register-source Loopback0
```

**Step 6** Use the **ip pim rp-address** command to statically configure a PIM rendezvous point (RP) for a multicast group.

```
Router(config)# ip pim rp-address 10.2.1.1 5 override
```

**Step 7** Follow these steps to configure the Ethernet backhaul interface.

- a. **interface type number**

```
interface VLAN2
```

- b. Use the **ip pim sparse-mode** command to enable PIM on the interface. You must use sparse mode.

```
Router(config-if)# ip pim sparse-mode
```

- c. Use the **ip pim query-interval** command to configure the frequency of Protocol Independent Multicast (PIM) query (hello) messages.

```
Router(config-if)# ip pim query-interval 2
```

- d. If you want to enable only the Protocol Independent Multicast (PIM) version 2 on the interface, use the **no ip pim version 1** command to disable PIM version 1.

```
Router(config-if)# no ip pim version 1
```

**Step 8** To configure which version of Internet Group Management Protocol (IGMP) the router uses, use the **ip igmp version** command.

```
Router(config-if)# ip igmp version 3
```

**Step 9** Exit the backhaul interface.

```
Router(config-if)# exit
Router(config)#
```

**Step 10** Follow these steps to configure multicast on the Ethernet shorthaul interface.

a. Enter the Ethernet shorthaul interface.

```
Router(config)# interface vlan 3
Router(config-if)#
```

a. Use the **ip pim sparse-mode** command to enable PIM on the interface. You must use sparse mode.

```
Router(config-if)# ip pim sparse-mode
```

b. Use the **ip pim query-interval** command to configure the frequency of Protocol Independent Multicast (PIM) query (hello) messages.

```
Router(config-if)# ip pim query-interval 2
```

c. Use the **ip igmp query-max-response-time** command to configure the maximum response time advertised in Internet Group Management Protocol (IGMP) queries.

```
Router(config-if)# ip igmp query-max-response-time 5
```

d. Use the **ip pim version** command to configure the Protocol Independent Multicast (PIM) version of the interface.

```
Router(config-if)# ip pim version 2
```

e. **Exit configuration mode.**

```
Router(config-if)# end
```

To verify your IP Multicast configuration, see [Verifying a Multicast Configuration](#). For more information about configuring Multicast, see the [Cisco IOS IP Multicast Configuration Guide, Release 12.2SR](#).

**Note**

The Cisco MWR 2941 does not support all of the commands described in the Cisco IOS Release 12.2SR documentation.

## Configuring Source-Specific Multicast

Source Specific Multicast (SSM) is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (not shared trees) are created.

Follow these steps to configure source-specific multicast (SSM).

**Step 1** Enter enable mode.

```
Router> enable
```

**Step 2** Enter configuration mode.

```
Router# configure terminal
```



**Step 3** Complete the following steps to create an access list to permit specific Multicast Groups for use with source-specific multicast configuration.

- a. Use the **ip access-list** command to define a standard IP access list.

```
Router(config)# ip access-list standard SSM
```

- b. Use the **permit** to allow traffic from multicast groups. Repeat this step for each network from which you want to allow traffic.

```
Router(config)# permit 239.193.0.0 0.0.255.255
Router(config)# permit 239.194.0.0 0.0.255.255
```

**Note**

For more information about using access control lists (ACLs), see [Creating an IP Access List and Applying It to an Interface](#).

**Step 4** Use the **ip multicast-routing** command to enable IP multicast routing. You can use the **distributed** keyword to enable Multicast Distributed Switching.

```
Router(config)# ip multicast-routing
```

**Step 5** Use the **ip pim ssm** command to configure SSM service. You can use the following keywords.

- The **default** keyword defines the SSM range access list as 232/8.
- The **range** keyword specifies the standard IP access list number or name that defines the SSM range.

```
Router(config)# ip pim ssm range SSM
```

**Step 6** Use the **ip pim register-source** command to configure the IP source address of a register message to an interface address other than the outgoing interface address of the designated router (DR) leading toward the rendezvous point (RP).

```
Router(config)# ip pim register-source Loopback0
```

**Step 7** Follow these steps to configure the Ethernet backhaul interface.

- a. Enter the VLAN interface.

```
interface VLAN2
```

- b. Use the **ip pim sparse-mode** command to enable PIM on the interface. You must use sparse mode.

```
Router(config-if)# ip pim sparse-mode
```

- c. Use the **ip pim query-interval** command to configure the frequency of Protocol Independent Multicast (PIM) query (hello) messages.

```
Router(config-if)# ip pim query-interval 2
```

- d. Use the **ip pim version** command to configure the Protocol Independent Multicast (PIM) version of the interface.

```
Router(config-if)# ip pim version 2
```

**Step 8** To configure which version of Internet Group Management Protocol (IGMP) the router uses, use the **ip igmp version** command.

```
Router(config-if)# ip igmp version 3
```

**Step 9** Follow these steps to configure the Ethernet shorthaul interface.

- e. Use the **ip pim sparse-mode** command to enable PIM on the interface. You must use sparse mode.

```
Router(config-if)# ip pim sparse-mode
```

- f. Use the **ip pim query-interval** command to configure the frequency of Protocol Independent Multicast (PIM) query (hello) messages.

```
Router(config-if)# ip pim query-interval 2
```

- g. Use the **ip igmp query-max-response-time** command to configure the maximum response time advertised in Internet Group Management Protocol (IGMP) queries.

```
Router(config-if)# ip igmp query-max-response-time 5
```

- h. Use the **ip pim version** command to configure the Protocol Independent Multicast (PIM) version of the interface.

```
Router(config-if)# ip pim version 2
```

- i. Use the **ip pim bsr-border** command to prevent bootstrap router (BSR) messages from being sent or received through an interface.

```
Router(config-if)# ip pim bsr-border
```

- j. Use the **ip igmp static-group** command to configure static group membership entries on an interface. When you configure the **ip igmp static-group** command, packets to the group are fast-switched out the interface, provided that packets were received on the correct reverse path forwarding (RPF) interface. Once configured, static group membership entries are added to the IGMP cache and mroute table.

```
Router(config-if)# ip igmp static-group 239.193.0.3 source 10.234.0.125
```

**Step 10** Exit configuration mode.

```
Router(config-if)# end
Router#
```

To verify your IP Multicast configuration, see [Verifying a Multicast Configuration](#). For more information about configuring Multicast, see the [Cisco IOS IP Multicast Configuration Guide, Release 12.2SR](#).



**Note**

The Cisco MWR 2941 does not support all of the commands described in the Cisco IOS Release 12.2SR documentation.

## Configuring Source Specific Multicast Mapping

SSM is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for audio and video broadcast application environments.

The Cisco MWR 2941 supports two types of SSM mapping.

- Static SSM Mapping—SSM static mapping enables you to configure the last hop router to use a static map to determine the sources sending to groups. Static SSM mapping requires that you configure access lists (ACLs) to define group ranges. The groups permitted by those ACLs then can be mapped to sources using the **ip igmp static ssm-map** command. To configure static SSM mapping, see [Configuring Static SSM Mapping](#).

- **DNS-Based SSM Mapping**—DNS-based SSM mapping enables you to configure the last hop router to perform a reverse DNS lookup to determine sources sending to groups. When DNS-based SSM mapping is configured, the router constructs a domain name that includes the group address G and performs a reverse lookup into the DNS. The router looks up IP address resource records (IP A RRs) to be returned for this constructed domain name and uses the returned IP addresses as the source addresses associated with this group. SSM mapping supports up to 20 sources for each group. The router joins all sources configured for a group. To configure DNS-based SSM mapping, see [Configuring DNS-Based SSM Mapping](#).

## Configuring Static SSM Mapping

Static SSM Mapping allows the the last hop router in an SSM deployment to determine the IP addresses of sources sending to groups. Follow these steps to configure static SSM mapping on the Cisco MWR 2941.

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Enter enable mode.<br><br>Router> enable  |
| <b>Step 2</b> | Enter configuration mode.<br><br>Router# configure terminal<br>Router(config)#  |
| <b>Step 3</b> | Use the <b>ip igmp ssm-map enable</b> command to enable SSM mapping for groups in the configured SSM range.<br><br>Router(config)# ip igmp ssm-map enable   |
| <b>Step 4</b> | If you want use static SSM mapping exclusively, use the <b>no ip igmp ssm-map query dns</b> command to disable DNS-based SSM mapping.<br><br>Router(config)# no ip igmp ssm-map query dns   |
| <b>Step 5</b> | Use the <b>ip igmp ssm-map static</b> command to configure a static SSM mapping entry.<br><br>Router(config)# ip igmp ssm-map static 11 172.16.8.11<br><br>If you want to configure additional static SSM mappings, repeat this step. |

## Configuring DNS-Based SSM Mapping

DNS-based SSM mapping allows the last hop router to perform DNS lookups to learn the IP addresses of sources sending to a group. Follow these steps to configure DNS-based SSM mapping.

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Enter enable mode.<br><br>Router> enable  |
| <b>Step 2</b> | Enter configuration mode.<br><br>Router# configure terminal<br>Router(config)#  |
| <b>Step 3</b> | Use the <b>ip igmp ssm-map enable</b> command to enable SSM mapping for groups in a configured SSM range.<br><br>Router(config)# ip igmp ssm-map enable |

- Step 4** Use the **ip igmp ssm-map query dns** command to enable DNS-based SSM mapping. By default, the **ip igmp ssm-map** command enables DNS-based SSM mapping.

```
Router(config)# ip igmp ssm-map query dns
```

- Step 5** Use the **ip domain multicast** command to specify the domain prefix used for DNS-based SSM mapping. The Cisco IOS software uses the ip-addr.arpa domain prefix by default.

```
Router(config)# ip domain multicast ssm-map.cisco.com
```

- Step 6** Use the **ip name-server** command to specify the address of one or more name servers to use for name and address resolution.

```
Router(config)# ip name-server 10.48.81.21
```

Repeat this step to configure additional DNS servers for redundancy, if required.

### Configuring Static Traffic Forwarding with SSM Mapping

You can use static traffic forwarding in conjunction with SSM mapping to statically forward SSM traffic for certain groups. When static traffic forwarding with SSM mapping is configured, the last hop router uses DNS-based SSM mapping to determine the sources associated with a group. The resulting (S, G) channels are then statically forwarded.

Follow these steps to configure static traffic forwarding with SSM mapping.

- Step 1** Enter enable mode.

```
Router> enable
```

- Step 2** Enter configuration mode.

```
Router# configure terminal
Router(config)#
```

- Step 3** Use the **interface** command to specify the interface on which to statically forward traffic for a multicast group using SSM mapping and enter interface configuration mode.

```
Router(config)# interface Vlan600
Router(config-if)#
```

- Step 4** Use the **ip igmp static-group** command to configure SSM mapping to be used to statically forward a (S, G) channel out of the interface. Use this command if you want to statically forward SSM traffic for certain groups, but you want to use DNS-based SSM mapping to determine the source addresses of the channels.

```
Router(config-if)# ip igmp static-group 232.1.2.1 source ssm-map
```

To verify your IP Multicast configuration, see [Verifying a Multicast Configuration](#). For more information about configuring Multicast, see the [Cisco IOS IP Multicast Configuration Guide, Release 12.2SR](#).



#### Note

The Cisco MWR 2941 does not support all of the commands described in the Cisco IOS Release 12.2SR documentation.

## Configuring Multicast VPN

The Multicast VPN Extranet Support feature enables service providers to distribute IP multicast content originated from one enterprise site to other enterprise sites. This feature enables service providers to offer the next generation of flexible extranet services, helping to enable business partnerships between different enterprise VPN customers. Using this feature, service providers can offer multicast extranet contracts to meet various business partnership requirements, including short-term, annual, and rolling contracts.

Follow these steps to configure a Multicast VPN on the Cisco MWR 2941.

- 
- Step 1** Enter enable mode.
- ```
Router> enable
```
- Step 2** Enter configuration mode.
- ```
Router# configure terminal
Router(config)#
```
- Step 3** Use the **ip multicast-routing** command to enable multicast routing.
- ```
Router(config)# ip multicast-routing
```
- Step 4** Use the **ip multicast-routing vrf** command to specify a Multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
- ```
Router(config)# ip multicast-routing vrf vrf1
```
- Step 5** Use the **ip vrf** command to enter VRF configuration mode and define the VPN routing instance by assigning a VRF name.
- ```
Router(config)# ip vrf vrf1
```
- Step 6** Use the **rd** command to create routing and forwarding tables. Specify the *route-distinguisher* argument to add an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter an RD in either of these formats:
- 16-bit autonomous system (AS) number: your 32-bit number, for example, 101:3
  - 32-bit IP address: your 16-bit number, for example, 192.168.122.15:1
- ```
Router(config-vrf)# rd 55:2222
```
- Step 7** Use the **route-target** command to create a route-target extended community for a VRF.
- The **import** keyword imports routing information from the target VPN extended community.
  - The *route-target-ext-community* argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.
- For content to be distributed from the source MVRF to the receiver MVRF, you must configure the same unicast routing policy on the source and receiver PE routers to import routes from the source VRF to the receiver VRF.
- ```
Router(config-vrf)# route-target import 55:1111
```
- Step 8** Use the **mdt default** command to configure a multicast group address range for data multicast distribution tree (MDT) groups for a VRF. A tunnel interface is created as a result of this command; by default, the destination address of the tunnel header is the *group-address* argument.
- ```
Router(config-vrf)# mdt default 232.3.3.3
```

- Step 9** Use the **route-target import** command to create a route-target extended community for a VRF.
- The **import** keyword imports routing information from the target VPN extended community.
  - The *route-target-ext-community* argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.
- For content to be distributed from the source MVRF to the receiver MVRF, you must configure the same unicast routing policy on the source and receiver PE routers to import routes from the source VRF to the receiver VRF.

```
Router(config-vrf)# route-target import 55:1111
```

- Step 10** Use the **mdt data** command to configure the multicast group address range for data MDT groups.
- This command configures a range of alternative multicast destination addresses for the tunnel header. The destination address chosen depends on the traffic profile (that is, the source and destination match the specified access list and the rate of the traffic has exceeded the bandwidth threshold value).
  - The threshold is in kbps.

```
Router(config-vrf)# mdt data 232.0.1.0 0.0.0.255 threshold 500 list 101
```

- Step 11** Use the **router bgp** command to enter router configuration mode create a BGP routing process.

```
Router(config)# router bgp 65535
```

- Step 12** Use the **address-family ipv4** command to create an IP MDT address family session.

```
Router(config-router)# address-family ipv4 mdt
```

- Step 13** Use the **neighbor activate** command to enter address family configuration to create an IP MDT address family session.

```
Router(config-router-af)# neighbor 192.168.1.1 activate
```

- Step 14** Use the **neighbor send-community** command to enable the MDT address family for this neighbor.

```
Router(config-router-af)# neighbor 192.168.1.1 send-community extended
```

- Step 15** Exit router configuration mode.

```
Router(config-router-af)# exit
Router(config)#
```

- Step 16** Use the **address-family** command to enter address family configuration mode to create a VPNv4 address family session.

```
Router(config-router)# address-family vpnv4
```

- Step 17** Use the **neighbor activate** command to enable the VPNv4 address family for this neighbor.

```
Router(config-router-af)# neighbor 192.168.1.1 activate
```

- Step 18** Use the **neighbor send-community** command to enable community and (or) extended community exchange with the specified neighbor.

```
Router(config-router-af)# neighbor 192.168.1.1 send-community extended
```

To verify your IP Multicast configuration, see [Verifying a Multicast Configuration](#). For more information about configuring Multicast, see the [Cisco IOS IP Multicast Configuration Guide, Release 12.2SR](#).

**Note**

The Cisco MWR 2941 does not support all of the commands described in the Cisco IOS Release 12.2SR documentation.

## Verifying a Multicast Configuration

You can use the following commands to verify your configuration.

- **show hosts**—Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular Domain Name System (DNS) view or for all configured DNS views.
- **show ip igmp groups** [*group-name* | *group-address* | *interface-type interface-number*] [**detail**]—Displays the multicast groups having receivers that are directly connected to the router and that were learned through IGMP. A receiver must be active on the network at the time that this command is issued in order for receiver information to be present on the resulting display.
- **show ip igmp ssm-mapping**—Display information about Source Specific Multicast (SSM) mapping or the sources that SSM mapping uses for a particular group.
- **show ip mroute** [**vrf** *vrf-name*] *group-address*—Displays the contents of the IP multicast routing table.
- **show ip msdp** [**vrf** *vrf-name*] **peer** [*peer-address* | *peer-name*]—Displays detailed information about Multicast Source Discovery Protocol (MSDP) peers.
- **show ip msdp** [**vrf** *vrf-name*] **summary**—Displays Multicast Source Discovery Protocol (MSDP) peer status.
- **show ip pim** [**vrf** *vrf-name*] **mdt bgp**—Shows details about the Border Gateway Protocol (BGP) advertisement of the route distinguisher (RD) for the multicast distribution tree (MDT) default group.
- **show ip pim mdt history**—Displays information about the history of data multicast distribution tree (MDT) groups that have been reused.
- **show ip pim** [**vrf** *vrf-name*] **mdt send**—To display the data multicast distribution tree (MDT) groups in use.
- **show ip pim rp** [**mapping**] [*rp-address*]—Displays RPs known in the network and shows how the router learned about each RP.
- **show mls ip multicast group** *group-address*—Displays MLS IP information.

For more information about how to configure IP Multicast on the Cisco MWR 2941, see the [Cisco IOS IP Multicast Configuration Guide, Release 12.2SR](#).

## Configuring Pseudowire

This section describes how to configure pseudowire on the Cisco MWR 2941. For an overview of pseudowire, see “[Cisco Pseudowire Emulation Edge-to-Edge](#)” section on page 1-3.

The Cisco MWR 2941 supports pseudowire connections using SAToP, CESoPSN, and ATM over MPLS. The following sections describe how to configure pseudowire connections on the Cisco MWR 2941.

- [Using Pseudowire Classes](#)
- [Using CEM Classes](#)

- [Configuring GRE Tunneling](#)
- [Using Pseudowire Labels](#)
- [Configuring a Backup Peer](#)
- [Configuring Structure-Agnostic TDM over Packet \(SAToP\)](#)
- [Configuring Circuit Emulation Service over Packet-Switched Network \(CESoPSN\)](#)
- [Configuring Transportation of Service Using ATM over MPLS](#)
- [Configuring Transportation of Service Using Ethernet over MPLS](#)

For full descriptions of each command, see [Appendix B, “Cisco MWR 2941 Router Command Reference.”](#) For pseudowire configuration examples, see [Appendix A, “Sample Configurations.”](#)

## Using Pseudowire Classes

A pseudowire class allows you to create a single configuration template for multiple pseudowire connections. You can apply pseudowire classes to all pseudowire types. Follow these steps to configure a pseudowire class:

---

**Step 1** Enter the following commands to create the pseudowire class.

- a. Enter configuration mode.

```
Router# configure terminal
```

- b. Use the **pseudowire-class** command to create a new pseudowire class.

```
Router(config)# pseudowire-class newclass
```

- c. Use the **encapsulation** command to set an encapsulation type. Use MPLS encapsulation for ATM over MPLS.

```
Router(config-pw-class)# encapsulation mpls
```

- d. Use the **mpls experimental** command to specify the 3-bit EXP field in the MPLS label used for pseudowire packets.

```
Router(config-pw-class)# mpls experimental 5
```



**Note**

---

For more information about the **mpls experimental** command, see [Appendix B, “Cisco MWR 2941 Router Command Reference.”](#)

---

- e. If there are multiple paths that traffic can cross within the pseudowire class, use the **preferred-path** command to specify a preferred path.

```
Router(config-pw-class)# preferred-path peer 50.0.0.1
```



**Note**

---

This command only applies to MPLS pseudowires.

---

**Step 2** Follow these steps to create a reference to the pseudowire class in the ATM IMA interface.

- a. Configure the pseudowire interface that you want to use the new pseudowire class. This example shows an ATM IMA interface.

```
Router(config)# interface atm0/ima0
```



```
Router(config-if)# pvc 0/40 l2transport
Router(cfg-if-atm-l2trans-pvc)# encapsulation aal0
```

- b. Use the **xconnect** command to bind an attachment circuit to the ATM IMA interface to create an ATM pseudowire. Use the **pw-class** parameter to specify the pseudowire class that the ATM pseudowire interface uses.

```
Router(cfg-if-atm-l2trans-pvc)# xconnect 1.1.1.1 40 pw-class myclass
```

**Note**

You cannot use the encapsulation **mpls** parameter with the **pw-class** parameter.

**Note**

The use of the **xconnect** command can vary depending on the type of pseudowire you are configuring.

## Using CEM Classes

A CEM class allows you to create a single configuration template for multiple CEM pseudowires. Follow these steps to configure a CEM class:

**Note**

You cannot apply a CEM class to other pseudowire types such as ATM over MPLS.

**Step 1** Follow these steps to create the CEM class.

- a. Enter configuration mode.

```
Router# configure terminal
```

- b. Use the **class cem** command to create a new CEM class

```
Router(config)# class cem mycemclass
```

- c. Enter the configuration commands common to the CEM class. This example specifies a sample rate, payload size, dejitter buffer, and idle pattern.

```
Router(config-cem-class)# payload-size 512
Router(config-cem-class)# dejitter-buffer 10
Router(config-cem-class)# idle-pattern 0x55
```

- d. Type **exit** to return to the config prompt.

```
Router(config-cem-class)# exit
```

**Step 2** Follow these steps to create a reference to the CEM class in the CEM interface.

- a. Enter the following commands to configure the CEM interface that you want to use the new CEM class.

```
Router(config)# interface cem 0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# cem class mycemclass
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
```

**Note**

The use of the **xconnect** command can vary depending on the type of pseudowire you are configuring.

- b. Use the **exit** command to exit the CEM interface.

```
Router(config-if-cem)# exit  
Router(config-if)#
```

## Configuring GRE Tunneling

You can use GRE tunneling with CEsPSN and ATM over MPLS PWs. Follow these steps to configure GRE tunneling on a CEsPSN, ATM over MPLS, or Ethernet over MPLS PWs.



### Note

For more information about configuring MPLS, see the [“Configuring Multiprotocol Label Switching \(MPLS\)”](#) section on page 4-58.

- Step 1** Use the following commands to create a loopback interface.

```
Router(config)# interface Loopback0  
Router(config-if)# description Loopback for MPLS and PWE3  
Router(config-if)# ip address 10.10.10.1 255.255.255.255  
Router(config-if)# exit  
Router(config)#
```

- Step 2** Complete the following steps to configure a tunnel interface.

- a. Create a tunnel interface.

```
Router(config)# interface Tunnel13  
Router(config-if)#
```

- b. Assign an IP address to the tunnel interface.

```
Router(config-if)# ip address 9.9.9.9 255.255.255.0
```

- c. Use the **tunnel mode** command to configure the tunnel to use GRE encapsulation.

```
Router(config-if)# tunnel mode gre ip
```

- d. Use the **mpls ip** command to enable MPLS switching.

```
Router(config-if)# mpls ip
```

- e. Use the **tunnel source** command to specify a source address or interface for the tunnel interface.

```
Router(config-if)# tunnel source Vlan3
```

- f. Use the **tunnel destination** command to specify the tunnel’s destination IP address.

```
Router(config-if)# tunnel destination 3.3.3.3
```

- g. Exit the tunnel interface.

```
Router(config-if)# exit  
Router(config)#
```

- Step 3** Create a route from the loopback interface to the tunnel interface.



### Note

When using the **ip route** command to create a route to the tunnel interface, enter the name of the tunnel interface rather than the IP address of the tunnel.

```
Router(config)# ip route 10.10.10.2 255.255.255.255 Tunnel13
```

- Step 4** Use the **mpls ldp router-id** command with the **force** parameter to change the MPLS IP address to the loopback interface address.

```
Router(config)# mpls ldp router-id loopback0 force
```

- Step 5** Use the **xconnect** command to bind the CEM or ATM interface to the loopback interface.

#### CEM

```
interface CEM0/15
description CESoPSN
no ip address
cem 0
  xconnect 10.10.10.1 111 encapsulation mpls
```

#### ATM

```
interface ATM0/0
no ip address
scrambling-payload
no atm ilmi-keepalive
pvc 0/10 l2transport
encapsulation aal5
  xconnect 10.10.10.1 300 encapsulation mpls
```

For sample configurations using GRE tunneling, see [Appendix A, “Sample Configurations”](#). For more information about configuring MPLS, see the [Cisco IOS Multiprotocol Label Switching Configuration Guide, Release 12.2SR](#).

## Verifying a GRE Tunnel Configuration

You can use the following commands to verify a GRE tunnel configuration.

- **show interface tunnel**
- **show adjacency tunnel**
- **show interfaces tunnel**
- **show platform hardware winpath gre-tunnel**

## Using Pseudowire Labels

Follow these steps to configure static pseudowire labels.



#### Note

When implementing a static pseudowire label configuration, ensure that each side has the same MPLS label, control word, and MTU settings. These settings must match for the pseudowire connection to function properly.

- Step 1** Use the **mpls label range** command in global configuration mode to define a new MPLS label. The command has the following parameters.
- *minimum-value*—The value of the smallest label allowed in the label space. The default is 16.

- *maximum-value*—The value of the largest label allowed in the label space. The default is platform-dependent.
- **static**—(Optional) Reserves a block of local labels for static label assignments. If you omit the static keyword and the minimum-static-value and maximum-static-value arguments, no labels are reserved for static assignment.
- *minimum-static-value*—(Optional) The minimum value for static label assignments. There is no default value.
- *maximum-static-value*—(Optional) The maximum value for static label assignments. There is no default value.

```
Router(config)# mpls label range min-label max-label [static min-static-label-value
max-static-label-value]
```

- Step 2** Use the **xconnect** command to define a static pseudowire and enter pseudowire label configuration mode:

```
Router(config-if-xconn)# xconnect 20.20.1.2 50 encapsulation mpls manual
```

- Step 3** Use the **mpls label** command to apply an MPLS label to the pseudowire interface.

```
Router(config-if-xconn)# mpls label local-vc-label remote-vc-label
```

- Step 4** Use the **mpls control-word** command to enable or disable a control word on the pseudowire connection.

```
Router(config-if-xconn)# mpls control-word
```

You can use the **show mpls l2transport vc detail** and **ping mpls pseudowire** commands to verify your configuration.

## Configuring a Backup Peer

A backup peer provides a redundant pseudowire (PW) connection in the case that the primary PW loses connection; if the primary PW goes down, the Cisco MWR 2941 diverts traffic to the backup PW. Follow these steps to configure a backup peer.

- Step 1** Use the **backup peer** command to define the address and VC of the backup peer.

```
Router(config)# backup peer peer-router-ip-address vcid [pw-class pw-class name]
```

- Step 2** Use the **backup delay** command to specify the delay before the router switches pseudowire traffic to the backup peer VC.

```
Router(config)# backup delay enable-delay [disable-delay | never]
```

Where:

- *enable-delay*—The time before the backup PW takes over for the primary PW.
- *disable-delay*—The time before the restored primary PW takes over for the backup PW.
- **never**—Disables switching from the backup PW to the primary PW.

## Configuring Structure-Agnostic TDM over Packet (SAToP)

Follow these steps to configure SAToP on the Cisco MWR 2941.

- Step 1** Use the **controller** command to configure the T1 or E1 interface.

```
Router(config)# controller [T1|E1] 0/4
Router(config-controller)#
```

- Step 2** Use the **cem-group** command to assign channels on the T1 or E1 circuit to the circuit emulation (CEM) channel. This example uses the **unframed** parameter to assign all the T1 timeslots to the CEM channel.

```
Router(config-if)# cem-group 4 unframed
```

- Step 3** Enter the following commands to define a CEM group.

```
Router(config)# interface CEM0/4
Router(config-if)# no ip address
Router(config-if)# cem 4
```

- Step 4** Use the **xconnect** command to bind an attachment circuit to the CEM interface to create a pseudowire. This example creates a pseudowire by binding the CEM circuit 304 to the remote peer 30.30.2.304.

```
Router(config-if)# xconnect 30.30.30.2 304 encapsulation mpls
```



### Note

When creating IP routes with a pseudowire configuration, we recommend that you build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as **ip route 30.30.30.2 255.255.255.255 1.2.3.4**.

## Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN)

Follow these steps to configure CESoPSN on the Cisco MWR 2941.

- Step 1** Use the **controller** command to access the E1 or T1 controller.

```
Router(config)# controller [e1|t1] 0/0
Router(config-controller)#
```

- Step 2** Use the **mode** command to set the controller in asynchronous transfer mode (ATM) or channel-associated signaling (CAS) mode.

```
Router(config-controller)# mode {atm | cas}
```

- Step 3** Use the **cem-group** command to assign channels on the T1 or E1 circuit to the circuit emulation (CEM) channel. This example uses the **timeslots** parameter to assign specific timeslots to the CEM channel.

```
Router(config-controller)# cem-group 5 timeslots 1-24
```

- Step 4** Use the **exit** command to exit controller configuration.

```
Router(config-controller)# exit
Router(config)#
```

- Step 5** Use the following commands to define a CEM channel:

```
Router(config)# interface CEM0/5
Router(config-if-cem)# cem 5
```

```
Router(config-if-cem)# signaling inband-cas
```

- Step 6** Use the **xconnect** command to bind an attachment circuit to the CEM interface to create a pseudowire. This example creates a pseudowire by binding the CEM circuit 305 to the remote peer 30.30.30.2.

```
Router(config-if-cem)# xconnect 30.30.30.2 305 encapsulation mpls
```

**Note**

When creating IP routes with a pseudowire configuration, we recommend that you build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as **ip route 30.30.30.2 255.255.255.255 1.2.3.4**.

- Step 7** Use the **exit** command to exit the CEM interface.

```
Router(config-if-cem)# exit  
Router(config)#
```

## Configuring Transportation of Service Using ATM over MPLS

ATM over MPLS pseudowires allow you to encapsulate and transport ATM traffic across an MPLS network. This service allows you to deliver ATM services over an existing MPLS network.

The following sections describe how to configure transportation of service using ATM over MPLS:

- [Configuring the Controller](#)
- [Configuring an IMA Interface](#)
- [Configuring the ATM over MPLS Pseudowire Interface](#)
- [Optional Configurations](#)

**Note**

For sample configurations for ATM over MPLS, see the [“ATM over MPLS Configuration” section on page A-17](#).

### Configuring the Controller

Follow these steps to configure the controller.

- Step 1** Enter the **card type** command to configure IMA on an E1 or T1 interface.

```
Router(config)# card type e1 0 0
```

- Step 2** Specify the controller interface on which you want to enable IMA.

```
Router(config)# controller E1 0/4  
Router(config-controller)#
```

- Step 3** Set the clock source to internal.

```
Router(config-controller)# clock source internal
```

- Step 4** If you want to configure an ATM IMA backhaul, use the **ima-group** command to assign the interface to an IMA group. For a T1 connection, use the **no-scrambling-payload** to disable ATM-IMA cell payload scrambling; for an E1 connection, use the **scrambling-payload** parameter to enable ATM-IMA cell payload scrambling.

The follow command assigns the interface to IMA group 0 and enables payload scrambling.

```
Router(config-controller)# ima-group 0 scrambling-payload
```

**Note**

For more information about configuring IMA groups, see [Configuring ATM IMA](#). For more information about how to configure the backhaul connection, see [Configuring MLPPP Backhaul](#).

## Configuring an IMA Interface

If you want to use ATM IMA backhaul, follow these steps to configure the IMA interface.

**Step 1** Specify the slot location and port of IMA interface group.

```
Router(config-controller)# interface ATM slot/IMA group-number
```

- *slot*—Specifies the slot location of the ATM IMA port adapter.
- *group-number*—Specifies the group number of the IMA group.

For example, the following command specifies the slot number as 0 and the group number as 0:

```
Router(config-controller)# interface atm0/ima0  
Router(config-if)#
```

**Note**

To explicitly configure the IMA group ID for the IMA interface, you may use the optional **ima group-id** command. You cannot configure the same IMA group ID on two different IMA interfaces; therefore, if you configure an IMA group ID with the system-selected default ID already configured on an IMA interface, the system toggles the IMA interface to make the user-configured IMA group ID the effective IMA group ID. At the same, the system toggles the original IMA interface to select a different IMA group ID.

**Step 2** Disable the IP address configuration for the physical layer interface.

```
Router(config-if)# no ip address
```

**Step 3** Specify the ATM bandwidth as dynamic.

```
Router(config-if)# atm bandwidth dynamic
```

**Step 4** Disable the Interim Local Management Interface (ILMI) keepalive parameters.

```
Router(config-if)# no atm ilmi-keepalive
```

For more information about configuring IMA groups, see the [“Configuring ATM IMA”](#) section on page 4-53.

## Configuring the ATM over MPLS Pseudowire Interface

You can configure ATM over MPLS in several modes according to the needs of your network. Use the appropriate section according to the needs of your network.

- [Configuring N-to-1 VCC Cell Transport Pseudowire](#)—Maps multiple VCCs to a single pseudowire
- [Configuring N-to-1 VPC Cell Transport](#)—Maps multiple VPCs to a single pseudowire
- [Configuring ATM AAL5 SDU VCC Transport](#)—Maps a single ATM PVC to another ATM PVC
- [Configuring 1-to-1 VCC Cell Mode](#)—Maps a single VCC to a single pseudowire
- [Configuring a Port Mode Pseudowire](#)—Maps one physical port to a single pseudowire connection



### Note

When creating IP routes with a pseudowire configuration, we recommend that you build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as `ip route 1.1.1.1 255.255.255.255 1.2.3.4`.

### Configuring N-to-1 VCC Cell Transport Pseudowire

An N-to-1 VCC cell transport pseudowire maps one or more ATM virtual channel connections (VCCs) to a single pseudowire. Follow these steps to configure an N-to-1 pseudowire.

You can use the following methods to configure an N-to-1 VCC Cell Transport pseudowire.

- [Mapping a Single PVC to a Pseudowire](#)
- [Mapping multiple PVCs to a Pseudowire](#)

### Mapping a Single PVC to a Pseudowire

To map a single PVC to an ATM over MPLS pseudowire, apply the **xconnect** command at the PVC level. This configuration type only uses AAL0 encapsulation. Follow these steps to map a single PVC to an ATM over MPLS pseudowire.

- Configure the ATM IMA interface.

```
Router(config)# interface atm0/ima0
```

- Use the **pvc** command to define a PVC.

```
Router(config-if)# pvc 0/40
Router(cfg-if-atm-l2trans-pvc)#
```

- Use the **encapsulation** command to define the encapsulation type for the PVC.

```
Router(cfg-if-atm-l2trans-pvc)# encapsulation aal0
```

- Use the **xconnect** command to bind an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding PVC 40 to the remote peer 1.1.1.1.

```
Router(config-if)# xconnect 1.1.1.1 40 encapsulation mpls
Router(cfg-if-atm-l2trans-pvc-xconn)#
```

- Use the **end** command to exit configuration mode.

```
Router(cfg-if-atm-l2trans-pvc-xconn)# end
Router#
```



### Mapping multiple PVCs to a Pseudowire

To map a multiple PVCs to a single ATM over MPLS pseudowire, apply the **xconnect** command at the subinterface level. This configuration allows you to group pseudowires logically, such as by the BTS to which the pseudowire is connected. Follow these steps to map a multiple PVCs to an ATM over MPLS pseudowire.



#### Note

If you configure multiple PVCs on an N-to-1 subinterface pseudowire, you must use AAL0 encapsulation for all of the PVCs.



#### Note

When you configure a N-to-1 pseudowire, you can also use the **ignore-vpi-vci** parameter. This parameter sets the Cisco MWR 2941 to ignore the VPI/VCI value in the PW packet and rewrite the egress ATM cell header with VPI/VCI value of the locally configured (attachment side) PVC. For more information about the **xconnect** command and the **ignore-vpi-vci** parameter, see [Appendix B, “Cisco MWR 2941 Router Command Reference.”](#)

- a. Configure the ATM IMA interface.

```
Router(config)# interface atm0/ima0
```

- a. Enter the following command to create an ATM IMA multipoint subinterface.

```
Router(config-if)# interface atm 0/ima0.1 multipoint
Router(config-subif)#
```

- b. Use the **xconnect** command to bind an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 100 to the remote peer 1.1.1.1.

```
Router(config-subif)# xconnect 1.1.1.1 100 encapsulation mpls
Router(config-subif-xconn)#
```

- c. Use the **exit** command to exit the xconnect subinterface.

```
Router(config-subif-xconn)# exit
Router(config-subif)#
```

- d. Use the **pvc** command to map a PVC to a pseudowire.

```
Router(config-if)# pvc 0/40 12transport
Router(cfg-if-atm-12trans-pvc)#
```

- e. Use the **encapsulation** command to define the encapsulation type for the PVC.

```
Router(config-if-atm-vc)# encapsulation aal0
```

- f. Define additional PVCs as appropriate. We recommend that you include a description for each PVC

```
Router(config-if)# pvc 0/41 12transport
Router(cfg-if-atm-12trans-pvc)# encapsulation aal0
Router(cfg-if-atm-12trans-pvc)# description voice channel
Router(cfg-if-atm-12trans-pvc)# exit
Router(config-subif)# pvc 0/42 12transport
Router(cfg-if-atm-12trans-pvc)# enc aal0
Router(cfg-if-atm-12trans-pvc)# description data channel
```

### Configuring N-to-1 VPC Cell Transport

An N-to-1 VPC cell transport pseudowire maps one or more ATM virtual path connections (VPCs) to a single pseudowire. While the configuration is similar to 1-to-1 VPC cell mode, this transport method uses the N-to-1 VPC Pseudowire protocol and format defined in RFCs 4717 and 4446. Follow these steps to configure an N-to-1 VPC pseudowire.

---

**Step 1** Configure the ATM IMA interface.

```
Router(config)# interface atm0/ima0  
Router(config-if)#
```

**Step 2** Use the **atm pvp** command to map a PVP to a pseudowire

```
Router(config-if)# atm pvp 10 l2transport  
Router(cfg-if-atm-l2trans-pvp)#
```

**Step 3** Use the **xconnect** command to bind an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 305 to the remote peer 30.30.30.2.

```
Router(cfg-if-atm-l2trans-pvp)# xconnect 30.30.30.2 305 encapsulation mpls  
Router(cfg-if-atm-l2trans-pvp-xconn)#
```

**Step 4** Use the **end** command to exit configuration mode.

```
Router(cfg-if-atm-l2trans-pvp-xconn)# end  
Router#
```

---

### Configuring ATM AAL5 SDU VCC Transport

An ATM AAL5 SDU VCC transport pseudowire maps a single ATM PVC to another ATM PVC. Follow these steps to configure an ATM AAL5 SDU VCC transport pseudowire.

---

**Step 1** Configure the ATM IMA interface.

```
Router(config)# interface atm 0/ima0  
Router(config-if)#
```

**Step 2** Use the **pvc** command to configure a PVC and specify a VCI/VPI.

```
Router(config-if)# pvc 0/12 l2transport  
Router(cfg-if-atm-l2trans-pvc)#
```

**Step 3** Use the **encapsulation** command to set the PVC encapsulation type to AAL5.

```
Router(cfg-if-atm-l2trans-pvc)# encapsulation aal5
```

**Note**

---

You must use AAL5 encapsulation for this transport type.

---

**Step 4** Use the **xconnect** command to bind an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 125 to the remote peer 25.25.25.25.

```
Router(cfg-if-atm-l2trans-pvc)# xconnect 25.25.25.25 125 encapsulation mpls
```

### Configuring 1-to-1 VCC Cell Mode

A VCC 1-to-1 pseudowire allows you to map a single ATM VCC to a single pseudowire. You must use AAL0 encapsulation for this transport type. Follow these steps to configure a 1-to-1 pseudowire.

- 
- Step 1** Configure the ATM IMA interface.

```
Router(config)# interface atm 0/ima0  
Router(config-if)#
```

- Step 2** Use the **pvc** command to configure a PVC and specify a VCI/VPI.

```
Router(config-if)# pvc 0/12 12transport  
Router(cfg-if-atm-12trans-pvc)#
```

- Step 3** Use the **encapsulation** command to set the PVC encapsulation type to AAL0.

```
Router(cfg-if-atm-12trans-pvc)# encapsulation aal0
```



**Note**

You must use AAL0 encapsulation for this transport type.

---

- Step 4** Use the **xconnect** command to bind an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 125 to the remote peer 25.25.25.25.

```
Router(cfg-if-atm-12trans-pvc)# xconnect 25.25.25.25 125 encapsulation mpls one-to-one
```

---

### Configuring a Port Mode Pseudowire

A port mode pseudowire allows you to map an entire ATM interface to a single pseudowire connection. Follow these steps to configure a port mode pseudowire:

- 
- Step 1** Configure the ATM interface.

```
Router(config)# interface atm 0/ima0
```

- Step 2** Use the **xconnect** command to bind an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 200 to the remote peer 25.25.25.25.

```
Router(cfg-if)# xconnect 25.25.25.25 2000 encapsulation mpls
```

---

## Optional Configurations

You can apply the following optional configurations to a pseudowire link.

- [Configuring Cell Packing](#)
- [Configuring PVC Mapping](#)

### Configuring Cell Packing

Cell packing allows you to improve the efficiency of ATM-to-MPLS conversion by packing multiple ATM cells into a single MPLS packet. Follow these steps to configure cell packing.

- Step 1** Use the **atm mcpt-timers** command to define the three Maximum Cell Packing Timeout (MCPT) timers under an ATM interface. The three independent MCPT timers specify a wait time before forwarding a packet.

```
Router(config)# int atm1/0
Router(config-if)# atm mcpt-timers 1000 2000 3000
```

- Step 2** Use the **cell-packing** command to specify the maximum number of cells in PW cell pack and the cell packing timer that the Cisco MWR 2941 uses. This example specifies 20 cells per pack and the third MCPT timer.

```
Router(config)# pvc 0/11 l2transport
Router(cfg-if-atm-l2trans-pvc)# encapsulation aal0
Router(cfg-if-atm-l2trans-pvc)# cell-packing 20 mcpt-timer 3
```

### Configuring PVC Mapping

PVC mapping allows you to map PVCs from multiple cell site routers to equivalent PVCs on a single aggregation node.



#### Note

PVC mapping only applies to N-to-1 cell mode and port mode. You can achieve a similar effect for AAL 5SSDU mode and VCC one-to-one mode by configuring a pseudowire between two PVCs with different VPI/VCI values on two PEs.

The following example shows how to use the **pw-pvc** command to map the local PVCs 0/11 and 0/12 to the remote PVCs 0/11 and 0/12.

```
(config)# int atm1/0
(config-if)# xconnect 25.25.25.25 2000 encapsulation mpls
(config-if)# pvc 0/11 l2transport
(cfg-if-atm-l2trans-pvc)# encapsulation aal0
(cfg-if-atm-l2trans-pvc)# pw-pvc 1/11
(config-if)# pvc 0/12 l2transport
(cfg-if-atm-l2trans-pvc)# encapsulation aal0
(cfg-if-atm-l2trans-pvc)# pw-pvc 1/12
```

## Configuring Transportation of Service Using Ethernet over MPLS

Ethernet over MPLS PWs allow you to transport Ethernet traffic over an existing MPLS network. For an overview of Ethernet over MPLS PWs, see the [“Transportation of Service Using Ethernet over MPLS” section on page 1-4](#).

### Configuring VLAN Mode

An Ethernet over MPLS PW in VLAN mode creates a connection based on an existing VLAN ID on the Cisco MWR 2941.

- Step 1** Create the VLAN interface that you want to bind to a pseudowire.

```
Router(config)# interface vlan 100  
Router(config-if)#
```

- Step 2** Use the **xconnect** command to the ethernet port interface to an attachment circuit to create a pseudowire. This example uses virtual circuit (VC) 101 to uniquely identify the PW. Ensure that the remote VLAN is configured with the same VC.

```
Router(config-if)# xconnect 1.1.1.2 101 encapsulation mpls
```

- Step 3** Add the GigabitEthernet interface to the VLAN.

```
Router(config-if)# interface GigabitEthernet 0/1  
Router(config-if)# switchport trunk allowed vlan 100  
Router(config-if)# switchport mode trunk
```

- Step 4** Create a corresponding configuration on the remote router with the same VCID value. This configuration uses VCID 101.



**Note**

The Cisco MWR 2941 supports VLAN rewriting on EoMPLS PWs. If the two networks use different VLAN IDs, the router rewrites PW packets using the appropriate VLAN number for the local network.



**Note**

When creating IP routes with a pseudowire configuration, we recommend that you build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as **ip route 1.1.1.2 255.255.255.255 1.2.3.4**.



**Note**

For more information about configuring VLANs on the Cisco MWR 2941, see [Configuring Gigabit Ethernet Interfaces, page 4-4](#).

## Configuring Layer 3 Virtual Private Networks (VPNs)

Layer 3 VPNs allow you to establish VPNs in a routed environment, improving the flexibility and ease of maintenance of VPNs. For instructions on how to configure layer 3 VPNs, see the [Cisco IOS Multiprotocol Label Switching Configuration Guide, Release 12.2SR](#).

## Configuring Quality of Service (QoS)

The following sections describe how to configure the Quality of Service (QoS) features supported by the Cisco MWR 2941 router.

- [QoS Limitations](#)
- [Sample QoS Configuration](#)
- [Configuring Classification](#)
- [Configuring Marking](#)
- [Configuring Congestion Management](#)
- [Configuring Shaping](#)
- [Configuring Ethernet Trusted Mode](#)

### QoS Limitations

The Cisco MWR 2941 offers different QoS support according to the physical interface and traffic type. The following sections describe the limitations for each QoS capability on the Cisco MWR 2941.

- [General QoS Limitations](#)
- [Statistics Limitations](#)
- [Propagation Limitations](#)
- [Classification Limitations](#)
- [Marking Limitations](#)
- [Congestion Management Limitations](#)
- [Shaping Limitations](#)

### General QoS Limitations

The following general QoS limitations apply to the Cisco MWR 2941.

- You can create a maximum of 32 class maps including the class-default class map.
- You can create a maximum of 32 policy-maps.
- You can create only 1 priority class within a policy-map.
- QoS is not supported on VLAN interfaces.
- The following limitations apply to MLPPP interfaces:
  - Input MLPPP interfaces do not support QoS service policies.
  - You can apply only one output QoS service policy to an MLPPP interface.
  - You can create a maximum of 8 **match** statements within a class map in a service policy applied to an MLPPP interface.

- When applying or modifying any aspect of a service-policy on an MLPPP interface, you must shut down and re-enable the interface.
- You can create a maximum of 8 classes within a policy-map that is applied to an MLPPP interface. This number includes the default-class.
- You can have only 1 priority class within a policy-map applied to an MLPPP interface.
- The following limitations apply to GigabitEthernet interfaces:
  - You can apply a maximum of 3 different service policies to Gigabit Ethernet interfaces. The service policies must be of the same type: input, output, or control.
  - You can only use the class-default class for HQoS parent service policies applied to egress GigabitEthernet interfaces.

### Statistics Limitations

- Input service policies on the GigabitEthernet interface support statistics based on class map and in terms of packets. Statistics based on filters and statistics in terms of bytes or rates are not supported.
- Output MLPPP interfaces support QoS statistics.
- Output service policies on the GigabitEthernet interface do not support statistics.

### Propagation Limitations

The Cisco MWR 2941 has the following limitations when propagating QoS values between interfaces:

- The following limitations apply when traffic ingresses through a GigabitEthernet interface and egresses through a GigabitEthernet interface:
  - When traffic is routed at layer 3, the switch maps the CoS bits to the QoS group value. The QoS group is not propagated through the L3 network processor.
  - When traffic is switched at layer 2, the QoS group is propagated through the switch.
- The following limitations apply when traffic ingresses through any other interface type (host-generated, MLPPP, or HWIC) and egresses through the GigabitEthernet interface.
  - The Precedence bit value is propagated to the CoS bit. The CoS bit value is mapped 1:1 to the QoS group value.

See [Sample QoS Configuration, page 4-93](#) for a sample QoS configuration that accounts for propagation limitations on the Cisco MWR 2941.



**Note** For more information about QoS restrictions for individual interface cards, see the documentation for [Cisco Interface Cards](#).

### Classification Limitations

[Table 4-1](#) summarizes the values that you can use to classify traffic based on interface type. The values are parameters that you can use with the **match** command.

**Table 4-1 QoS Classification Limitations by Interface**

	GigabitEthernet		HWIC-9ESW		MLPPP		HWIC-1GE-SFP		HWIC-ADSL		HWIC-SHDSL	
Value	Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress
access-group												

**Table 4-1** QoS Classification Limitations by Interface (continued)

	GigabitEthernet	HWIC-9ESW	MLPPP	HWIC-1GE-SFP	HWIC-ADSL	HWIC-SHDSL
all						
any	X		X	X		
any						
class-map						
cos	X			X		
destination-address						
discard-class						
dscp	X		X	X		
flow pdp						
frde						
frdlci						
ip dscp	X			X		
ip precedence						
ip rtp						
mpls experimental			X	X		
not						
packet length						
precedence						
protocol						
qos-group		X				
source-address						
vlan	X					

The following limitations also apply when configuring classification on the Cisco MWR 2941.

- The following limitations apply to input Gigabit Ethernet interface QoS policies:
  - You can use a the **match vlan** command with a maximum of 4 VLANs.
  - You can use the **match dscp** command with a maximum of 4 DSCP values.
  - You cannot use the same match statement more than once in a single class map. For example, you cannot add two **match vlan** commands to a single class map.
  - You cannot use the **match cos** and **match dscp** commands together in a single class map.
- The following limitations apply to output Gigabit Ethernet interface QoS policies:
  - Class maps only support matching based on qos-group. This limitation does not apply to the class-default class map.
  - You cannot create two policy maps that match based on the same qos-group value.



- The following limitations apply to input MLPPP interfaces:
  - You can create up to 8 matches in a class-map using DSCP or MPLS Exp values.

## Marking Limitations

Table 4-2 summarizes the values that you can use to mark traffic based on interface type. The values are parameters that you can use with the **set** command.

**Table 4-2 QoS Marking Limitations by Interface**

	GigabitEthernet		HWIC-9ESW		MLPPP		HWIC-1GE-SFP		HWIC-ADSL		HWIC-SHDSL	
Value	Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress
atm-clp												
cos	X		X									
discard-class												
dscp												
dscp-transmit												
ip dscp	X											
ip precedence												
mpls experimental												
mpls experimental imposition												
mpls experimental imposition qos-group												
precedence												
prec-transmit												
qos-group	X											

## Congestion Management Limitations

The congestion management limitations for the Cisco MWR 2941 are described in the following sections:

- [Queuing Limitations](#)
- [Rate Limiting Limitations](#)

### Queuing Limitations

The Cisco MWR 2941 uses Class-based fair weighted queuing (CBFQ) for congestion management. [Table 4-3](#) summarizes the queuing commands that you can apply when using CBFQ according to interface type.

**Table 4-3** *QoS Queuing Limitations by Interface*

	GigabitEthernet		HWIC-9ESW		MLPPP		HWIC-1GE-SFP		HWIC-ADSL		HWIC-SHDSL	
Value	Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress
bandwidth (kbps)												
bandwidth percent		X				X						
bandwidth remaining percent		X	X			X						
compression header ip												
drop												
fair-queue												
priority		X				X						
priority (kbps)												
priority (without queue-limit)												
priority percent		X				X						
queue-limit (cells)												
queue-limit (packets)		X				X						

### Rate Limiting Limitations

You can use rate limiting for congestion management on the Cisco MWR 2941. [Table 4-4](#) summarizes the rate limiting parameters that you can use with the **police** command according to interface type. The table uses the following terms:

- **Rate**—A speed of network traffic such as a committed information rate (CIR) or peak information rate (PIR).
- **Actions**—A defined action when traffic exceeds a rate, such as conform-action, exceed-action, or violate-action.

**Table 4-4 QoS Rate Limiting Limitations by Interface**

	GigabitEthernet		HWIC-9ESW		MLPPP		HWIC-1GE-SFP		HWIC-ADSL		HWIC-SHDSL	
<b>Policing with</b>	Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress
One rate												
One rate and two actions								X		X		X
Two rates and two actions												
Two rates and three actions												

**Shaping Limitations**

Table 4-5 summarizes the values that you can use to mark traffic based on interface type. The values are parameters that you can use with the **shape** command.

**Table 4-5 QoS Shaping Limitations by Interface**

	GigabitEthernet		HWIC-9ESW		MLPPP		HWIC-1GE-SFP		HWIC-ADSL		HWIC-SHDSL	
<b>Value</b>	Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress
adaptive												
average		X						X		X		X
fecn-adapt												
max-buffers												
peak												

The following limitations also apply to QoS shaping on the Cisco MWR 2941:

- The following limitations apply to input Gigabit Ethernet interfaces:
  - You cannot apply shaping to the class-default class unless you are using hierarchical policy maps and applying shaping to the parent policy map.
  - If you are using hierarchical policy maps, you can only apply the class-default class to the parent policy map.

**Sample QoS Configuration**

The following configuration demonstrates how to apply QoS given the hardware limitations. The Cisco MWR 2941 processes traffic between interfaces as follows:

- For layer 2 traffic passing between the GigabitEthernet 0/2 interface and the GigabitEthernet 0/0 interface, the output queue is determined by the QoS Group assigned in the in-qos policy map.
- For layer 3 traffic passing between GigabitEthernet 0/2 interface and the GigabitEthernet 0/0 interface, the output queue is determined based on the CoS value assigned in the in-qos policy map. (the CoS value is mapped 1:1 to the QoS group value.)

- For traffic passing between other interfaces, the output queue is determined based on the CS fields (top three bits) of the IP DSCP bits; these bits are copied to the CoS bits, which are mapped 1:1 to the QoS group value.

```

!
class-map match-all q0
  match qos-group 0
class-map match-all q1
  match qos-group 1
class-map match-all q2
  match qos-group 2
class-map match-all q3
  match qos-group 3
class-map match-all q4
  match qos-group 4
class-map match-all q5
  match qos-group 5
class-map match-all q6
  match qos-group 6
class-map match-all q7
  match qos-group 7
class-map match-any Voice
  match dscp ef
class-map match-any Signaling
  match dscp af41
class-map match-any HSDPA
  match dscp af11 af12
!
policy-map in-qos
  class Voice
    set cos 5
    set qos-group 5
  class control_plane
    set cos 4
    set qos-group 4
  class HSDPA
    set cos 1
    set qos-group 1
!
policy-map out-child
  class q5
    priority percent 20
  class q4
    bandwidth remaining percent 20
  class q1
    bandwidth remaining percent 59
!
!
policy-map out-parent
  class class-default
    shape average 100000000
    service-policy out-child
!
interface GigabitEthernet 0/2
  switchport access vlan 20
  service-policy input in-qos
!
interface GigabitEthernet 0/0
  switchport trunk allowed vlan 1,10-30,1002-1005
  switchport mode trunk
  service-policy output out-parent

```

**Note**

This is a partial configuration intended to demonstrate the QoS feature.

To view other QoS sample configurations see [Appendix A, “Sample Configurations”](#).

## Configuring Classification

Classifying network traffic allows you to organize packets into traffic classes based on whether the traffic matches specific criteria. Classifying network traffic is the foundation for enabling many QoS features on your network.

### Creating a Class Map for Classifying Network Traffic

Class maps allow you to define classes of network traffic in order to apply QoS features to each class. Follow these steps to create a class map.

- Step 1** Enter enable mode.

```
Router> enable
```

- Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

- Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

- Step 4** Use the **class-map** command to define a new class map and enter class map configuration mode.

```
Router(config)# class-map class1
```

- Step 5** Use the **match** command to specify the match criteria for the class map. You can define a variety of match criteria including CoS, DSCP, MPLS Exp, or QoS group value.

```
Router(config-cmap)# match qos-group 7
```

- Step 6** Exit configuration mode.

```
Router(config-cmap)# end
Router#
```

### Creating a Policy Map for Applying a QoS Feature to Network Traffic

A policy map allows you to apply a QoS feature to network traffic based on the traffic classification. Follow these steps to create and configure a policy map that uses an existing class map.

- Step 1** Enter enable mode.

```
Router> enable
```

- Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

- Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

- Step 4** Use the **policy-map** command to define a new policy map and enter policy map configuration mode.

```
Router(config)# policy-map policy1  
Router(config-pmap)#
```

- Step 5** Use the **class** command to specify a traffic class to which the policy applies. This command enters policy-map class configuration mode, which allows you to define the treatment for the traffic class.

```
Router(config-pmap)# class class1  
Router(config-pmap-c)#
```

Use the **bandwidth** command to specify the bandwidth allocated for a traffic class attached to the policy map. You can define the amount of bandwidth in kbps, a percentage of bandwidth, or an absolute amount of bandwidth. This step is optional.



---

**Note** GigabitEthernet interfaces only support bandwidth defined as a percentage or remaining percent.

---

```
Router(config-pmap-c)# bandwidth percent 50
```

- Step 6** Exit configuration mode.

```
Router(config-cmap)# end  
Router#
```



---

**Note** You can use the **show policy-map** command to verify your configuration.

---

## Attaching the Policy Map to an Interface

After you create the policy map, you must attach it to an interface. Policy maps can be attached to either the input or output direction of the interface.

- 
- Step 1** Enter enable mode.

```
Router> enable
```

- Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

- Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Step 4** Specify the interface to which you want to apply the policy map.

```
Router(config)# interface gigabitEthernet0/1
```

**Step 5** Use the **service-policy** command to attach the policy map to an interface. The **input** and **output** parameters specify the direction in which router applies the policy map.

```
Router(config-if)# service-policy output policy1
```

**Step 6** Exit configuration mode.

```
Router(config-cmap)# end  
Router#
```

**Note**

You can use the **show policy map** interface command to verify your configuration.

For more information about configuring classification, see the [Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2SR](#).

## Configuring Marking

Marking network traffic allows you to set or modify the attributes for packets in a defined traffic class. You can use marking with traffic classification to configure variety of QoS features for your network.

The Cisco MWR 2941 marking allows you to modify the following packet attributes:

- Differentiated services code point (DSCP) value
- Class of service (CoS) value
- MPLS Exp bit value
- Qos-group value (internal)

For instructions on how to configure marking for IP Precedence, DSCP, or CoS value, use the following sections:

- [Creating a Class Map for Marking Network Traffic](#)
- [Creating a Policy Map for Applying a QoS Feature to Network Traffic](#)
- [Attaching the Policy Map to an Interface](#)

For instructions on how to configure MPLS Exp bit marking, see the “[Configuring MPLS Exp Bit Marking using a Pseudowire](#)” section on page 4-100.

### Creating a Class Map for Marking Network Traffic

Class maps allow you to define classes of network traffic in order to apply QoS features to each class. Follow these steps to define a traffic class to mark network traffic.

**Step 1** Enter enable mode.

```
Router> enable
```

**Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

**Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Step 4** Use the **class-map** command to define a new class map and enter class map configuration mode.

```
Router(config)# class-map class1
```

**Step 5** Use the **match** command to specify the match criteria for the class map. You can define a variety of match criteria including CoS, DSCP, MPLS Exp, or QoS group value.

```
Router(config-cmap)# match qos-group 7
```

**Step 6** Exit configuration mode.

```
Router(config-cmap)# end  
Router#
```

---

## Creating a Policy Map for Applying a QoS Feature to Network Traffic

Policy maps allow you to apply the appropriate QoS feature to the network traffic based on the traffic classification. The follow sections describe how to create and configure a policy map to use a class map or table map.

The following restrictions apply when applying a QoS feature to network traffic:

- A policy map containing the **set qos-group** command can only be attached as an output traffic policy.
- A policy map containing the **set cos** command can only be attached as an input traffic policy.

Follow these steps to create a policy map.

---

**Step 1** Enter enable mode.

```
Router> enable
```

**Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

**Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Step 4** Use the **policy-map** command to define a policy map and enter policy map configuration mode.

```
Router(config)# policy-map policy1  
Router(config-pmap)#
```

**Step 5** Use the **class** command to specify the traffic class for which you want to create a policy and enter policy map class configuration mode. You can also use the **class-default** parameter to define a default class.

```
Router(config-pmap)# class class1  
Router(config-pmap-c)#
```



**Step 6** Use one of the **set** commands listed in [Table 6](#) to define a QoS treatment type.

**Table 6** *set Commands Summary*

set Commands	Traffic Attributes	Network Layer	Protocol
<b>set cos</b>	Layer 2 CoS value of the outgoing traffic	Layer 2	ATM
<b>set dscp</b>	DSCP value in the ToS byte	Layer 3	IP
<b>set qos-group</b>	QoS group ID	Layer 3	IP, MPLS

**Step 7** Exit configuration mode.

```
Router(config-pmap) # end
Router#
```



**Note**

You can use the **show policy-map** or **show policy-map *policy-map* class *class-name*** commands to verify your configuration.

## Attaching the Policy Map to an Interface

**Step 1** Enter enable mode.

```
Router> enable
```

**Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

**Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Step 4** Specify the interface to which you want to apply the policy map.

```
Router(config)# interface gigabitEthernet0/1
```

**Step 5** Use the **service-policy** command to attach the policy map to an interface. The **input** and **output** parameters specify the direction in which router applies the policy map.

```
Router(config-if)# service-policy input policy1
```

**Step 6** Exit configuration mode.

```
Router(config-cmap) # end
Router#
```

**Note**

You can use the **show policy map** interface command to verify your configuration.

## Configuring MPLS Exp Bit Marking using a Pseudowire

You can also configure MPLS Exp bit marking within an ATM over MPLS pseudowire interface using the **mpls experimental** command. Follow these steps to configure MPLS Exp bit marking using a pseudowire interface.

**Step 1** Follow these steps to create a pseudowire class that sets an MPLS Exp value.

- a. Create a new pseudowire class.

```
Router(config)# pseudowire-class MPLS_3
```

- b. Configure MPLS encapsulation.

```
Router(config-pw-class)# encapsulation mpls
```

- c. Use the **mpls experimental** command to specify the MPLS Exp bit value.

```
Router(config-pw-class)# mpls experimental 3
```

- d. Use the **exit** command to exit the pseudowire-class interface.

```
Router(config-pw-class)# exit
Router(config)#
```

**Step 2** Complete the following steps to apply the pseudowire class to a pseudowire:

- a. Configure the ATM/IMA interface.

```
Router(config)# interface ATM0/IMA0
Router(config-if)#
```

- b. Specify a PVC.

```
Router(config-if)# pvc 2/1 12transport
Router(cfg-if-atm-12trans-pvc)#
```

- c. Specify an encapsulation type for the PVC.

```
Router(cfg-if-atm-12trans-pvc)# encapsulation aa10
```

- d. Use the **xconnect** command with the **pw-class** parameter to create a pseudowire that uses the configuration defined in the pseudowire class.

```
Router(cfg-if-atm-12trans-pvc)# xconnect 10.10.10.1 121 pw-class MPLS_3
```

For more information about configuring marking, see the [Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2SR](#).

**Note**

The Cisco MWR 2941 does not support all of the commands described in the IOS Release 12.2SR documentation.

## Configuring Congestion Management

The following sections describe how to configure congestion management on the Cisco MWR 2941.

- [Configuring Low Latency Queueing \(LLQ\)](#)
- [Configuring Class-Based Weighted Fair Queuing \(CBFQ\)](#)

### Configuring Low Latency Queueing (LLQ)

Low latency queuing allows you to define a percentage of bandwidth to allocate to an interface or PVC as a percentage. You can define a percentage for priority or nonpriority traffic classes. Follow these steps to configure LLQ.

---

**Step 1** Enter enable mode.

```
Router> enable
```

**Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

**Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Step 4** Use the **policy-map** command to define a policy map.

```
Router(config)# policy-map policy1
```

**Step 5** Use the **class** command to reference the class map that defines the traffic to which the policy map applies.

```
Router(config-pmap)# class class1
Router(config-pmap-c)#
```

**Step 6** Use the **priority** command to specify the priority percentage allocated to the traffic class assigned to the policy map. You can use the **burst** parameter to configure the network to accommodate temporary bursts of traffic.

```
Router(config-pmap-c)# priority percent 10
```

**Step 7** Use the **bandwidth** command to specify the bandwidth available to the traffic class within the policy map. You can specify the bandwidth in kbps or by a percentage of bandwidth.

```
Router(config-pmap-c)# bandwidth percent 30
```

**Step 8** Exit configuration mode.

```
Router(config-pmap-c)# end
Router#
```



**Note**

You can use the **show policy-map**, **show policy-map policy-map class class-name**, or **show policy-map interface** commands to verify your configuration.

---

## Configuring Class-Based Weighted Fair Queuing (CBFQ)

The Cisco MWR 2941 supports Class-Based Weighted Fair Queuing (CBWFQ) for congestion management. Follow these steps to configure CBWFQ.

**Step 1** A class map contains match criteria against which a packet is checked to determine if it belongs to the class. You can use class maps to define criteria that are referenced in one or more policy maps. Complete the following steps to configure a class map.

- a. Use the **class-map** command to create a class map.

```
Router(config)# class-map class1  
Router(config-cmap)#
```

- b. Use the **match** command to specify the match criteria for the class map. You can define a variety of match criteria including CoS, DSCP, MPLS Exp, or QoS group value.

```
Router(config-cmap)# match qos-group 7
```

- c. Use the **exit** command to exit class map configuration.

```
Router(config-cmap)# exit  
Router(config)#
```

**Step 2** Complete the following steps to configure a policy map and attach it to an interface.



**Note**

The Cisco MWR 2941 does not support the **random-detect** command.

- a. Use the **policy-map** command to define a policy map.

```
Router(config)# policy-map policy1  
Router(config-pmap)#
```

- b. Use the **class** command to reference the class map that defines the traffic to which the policy map applies.

```
Router(config-pmap)# class class1  
Router(config-pmap-c)#
```

- c. Use the **bandwidth** command to specify the bandwidth allocated for the traffic class.

```
Router(config-pmap-c)# bandwidth 3000
```

- d. Use the **exit** command to exit the policy map class configuration.

```
Router(config-pmap-c)# exit  
Router(config-pmap)#
```

- e. Use the **exit** command to exit the policy map configuration.

```
Router(config-pmap)# exit  
Router(config)#
```

- f. Enter configuration for the interface to which you want to apply the policy map.

```
Router(config)# interface atm0/ima0
```

- g. Use the **service-policy** command to apply the service policy to the interface.

```
Router(config-if)# service-policy output policy1
```

## Configuring Shaping

The Cisco MWR 2941 supports class-based traffic shaping. Follow these steps to configure class-based traffic shaping.

Class-based traffic shaping is configured using a hierarchical policy map structure; you enable traffic shaping on a primary level (parent) policy map and other QoS features such as queuing and policing on a secondary level (child) policy map.

The following sections describe how to configure shaping.

- [Configuring Class-Based Traffic Shaping in a Primary-Level \(Parent\) Policy Map](#)
- [Configuring the Secondary-Level \(Child\) Policy Map](#)

### Configuring Class-Based Traffic Shaping in a Primary-Level (Parent) Policy Map

Follow these steps to configure a parent policy map for traffic shaping.

- 
- Step 1** Use the **policy-map** command to specify the policy map for which you want to configure shaping and enter policy-map configuration mode.
- ```
Router(config)# policy-map output-policy
```
- Step 2** Use the **class** command to specify the traffic class to which the policy map applies.
- ```
Router(config-pmap)# class class1
Router(config-pmap-c)#
```
- Step 3** Use the **shape** command to define algorithm and rate used for traffic shaping.
- ```
Router(config-pmap-c)# shape [average | peak] mean-rate [[burst-size] [excess-burst-size]]
```
- Step 4** Use the **service-policy** command to attach the policy map to the class map.
- ```
Router(config-pmap-c)# service-policy policy-map
```
- Step 5** Exit configuration mode.
- ```
Router(config-pmap-c)# end
Router#
```

**Note**

You can use the **show policy-map** command to verify your configuration.

For more information about configuring shaping, see [Regulating Packet Flow on a Per-Class Basis---Using Class-Based Traffic Shaping](#).

**Note**

The Cisco MWR 2941 does not support all of the commands described in the IOS Release 12.2SR documentation.

## Configuring the Secondary-Level (Child) Policy Map

Follow these steps to create a child policy map for traffic shaping.

- Step 1** Use the **policy-map** command to specify the policy map for which you want to configure shaping and enter policy-map configuration mode.

```
Router(config)# policy-map output-policy
```

- Step 2** Use the **class** command to specify the traffic class to which the policy map applies.

```
Router(config-pmap)# class class1  
Router(config-pmap-c)#
```

- Step 3** Use the **bandwidth** command to specify the bandwidth allocated to the policy map. You can specify the bandwidth in kbps, a relative percentage of bandwidth, or an absolute amount of bandwidth.

```
Router(config-pmap-c)# bandwidth percent 50
```

- Step 4** Exit configuration mode.

```
Router(config-pmap-c)# end  
Router#
```

For more information about configuring shaping, see [Regulating Packet Flow on a Per-Class Basis---Using Class-Based Traffic Shaping](#).

**Note**

The Cisco MWR 2941 does not support all of the commands described in the IOS Release 12.2SR documentation.

## Configuring Ethernet Trusted Mode

The Cisco MWR 2941 supports trusted and non-trusted mode for switch ports. Switch ports are set in non-trusted mode by default; if you want to set the ethernet switch ports in trusted mode, use the global command **switch l2trust** to set all ethernet ports to trusted mode.

```
Router(config)# switch l2trust
```

For more information about the **switch l2trust** command, see the [Appendix B, "Cisco MWR 2941 Router Command Reference."](#)

## Configuring Link Noise Monitor

Noise on T1 and E1 links that span between the BTS and central office can affect voice quality for mobile users to the point where it becomes unacceptable. To monitor the quality of individual links in a multilink bundle, you can configure the Link Noise Monitor (LNM) on your Cisco MWR 2941 router.

The LNM detects, alerts, and removes noisy links from a bundle based on user-defined thresholds and durations. In addition, the LNM notifies the operator once the quality of the line has improved, and restores the link service if the link has been removed.

To detect noise on a link, the LNM monitors the following two types of errors which make up the Bit Error Rate (BER) and compares the number of errors with the user-defined thresholds:

- **Line Code Violation (LCV)**—A Bi-Polar Violation (BPV) or Excessive Zeroes (EXZ) error has occurred.
- **Path Code Violation (PCV)**—A Cyclic Redundancy Check (CRC) error, which is generally caused by one or more LCV or logic errors, has occurred in a time slot.

The LNM provides the following types of noise monitors:

- **Link Warning**—Issues a warning when the noise level of a link exceeds a user-defined threshold and notifies the operator when the noise level improves to the point that it drops below a second user-defined threshold.
- **Link Removal**—Issues an error and removes a link from service when the noise level of the link exceeds a user-defined threshold and restores the link and provides notification when the noise level improves to the point that it drops below a second user-defined threshold.



**Note**

If the noise level on the last active link in a multilink bundle exceeds the Link Removal threshold, an alert is issued but the link is not removed from service. If this situation occurs, the standard T1 error rate is used to determine if the last active link must be removed from service.

To configure the LNM feature, issue the **span** command from controller configuration mode of each T1 or E1 link in the bundle that you want to monitor. To disable LNM on a link, issue the **no** version of the command from controller configuration mode of the link.

```
span {warn | remove} [{lcv value [pcv value]} [duration seconds]} set | clear
```

where:

- **warn**—Enables Link Warning monitoring on the link.
- **remove**—Enables Link Removal monitoring on the link.
- **lcv value**—Threshold (in bit errors per second) that when exceeded for the configured duration when the **set** keyword has been specified, creates a condition (warning or link removal), or when fallen below for the configured duration when the **clear** keyword has been specified, clears the condition.

For T1 links:

- Valid range is 5 to 1544.
- For Link Warning monitoring, the default is 15.
- For Link Removal monitoring, the default is 154.

For E1 links,

- Valid range is 7 to 2048.
- For Link Warning monitoring, the default is 20.
- For Link Removal monitoring, the default is 205.
- **pcv value**—Number of time slots in errors per second. If not specified by the user, this value is calculated from the LCV threshold based on a Gaussian distribution that matches typical noise-induced errors.

For T1 links:

- Valid range is 3 to 320.
- For Link Warning monitoring, the default is 15.
- For Link Removal monitoring, the default is 145.

For E1 links:

- Valid range is 8 to 832.
- For Link Warning monitoring, the default is 20.
- For Link Removal monitoring, the default is 205.

- **duration seconds**—Number of seconds that a threshold must be exceeded to create a condition or fallen below to clear a condition. Valid range is 1 to 600. The default is 10.

When specified with the **lcv** keyword, the duration must be configured after the LCV threshold. For example, **span warn lcv 55 duration 20** is a correct way to issue the command; **span warn duration 20 lcv 55** is not.

- **set**—Specifies that the values configured for the **span** command are to be used to set a condition.
- **clear**—Specifies that the values configured for the **span** command are to be used to clear a condition.

## Usage Notes

When configuring the LNM, please note the following:

- If the **warn** and **remove** keywords are specified without any other options, the LCV and PCV thresholds and duration defaults are used to determine (**set**) and clear (**clear**) the condition.
- If the **span** command is issued with the **set** keyword specified (defining the LNM type and parameters to use to determine a condition exists) and the command is not issued again with the **clear** keyword specified (defining the parameters used to clear a condition), or vice versa, the values configured for the threshold and duration are used for both.
- If the **span** command is issued without either the **set** or **clear** keywords specified, **set** is the default.
- The **set** and **clear** keywords can only be specified if the threshold and/or duration has been specified.
- If the PCV threshold is not configured (using the **pcv** keyword and value), the threshold is calculated using Gaussian probability distribution that is representative of most noise environments.
- The following SYSLOG messages have been added for fault notification:
  - %LNM-4- WARNEXCEED:Controller <Controller IF>, exceeded noise warning threshold <int>, duration <int>
  - %LNM-4- WARNIMPROVE:Controller <Controller IF>, noise improved below threshold <int>, duration <int>
  - %LNM-2- REMOVE:Interface <Serial IF> removed, noise exceeded threshold <int>, duration <int>
  - %LNM-2- RESTORE:Interface <Serial IF> restored, noise improved below threshold <int>, duration <int>
  - %LNM-2- REMEXCEED:Interface <Serial IF>, noise exceeded threshold <int>, duration <int>
  - %LNM-2- REMIMPROVE:Interface <Serial IF>, noise improved below threshold <int>, duration <int>



## Saving Configuration Changes

After you have completed configuring your Cisco MWR 2941 router, to prevent the loss of the router configuration, you must store the configuration changes by saving it to NVRAM so that the router boots with the configuration you entered.

---

**Step 1** Exit the global configuration mode.

```
Router(config)# exit
```



**Tip**

To return immediately to enable mode (Router#), press **Ctrl-Z** in any mode instead of entering **exit**, which returns you to the mode you were in previously.

---

**Step 2** Save the configuration changes to NVRAM so that they are not lost during resets, power cycles, or power outages.

```
Router# copy running-config startup-config
```

---

## Monitoring and Managing the Cisco MWR 2941 Router

The following sections describe how to monitor and manage the Cisco MWR 2941:

- [Using Cisco Mobile Wireless Transport Manager \(MWTM\)](#)
- [Enabling Remote Network Management](#)
- [Show Commands for Monitoring the Cisco MWR 2941 Router](#)
- [Configuring Cisco Networking Services \(CNS\)](#)

## Using Cisco Mobile Wireless Transport Manager (MWTM)

You can use Cisco network management applications, such as Cisco Mobile Wireless Transport Manager (MWTM), to monitor and manage the Cisco MWR 2941. This Network Management tool provides monitoring and management capabilities to the RAN-O solution. The Cisco MWTM addresses the element-management requirements of mobile operators and provides fault, configuration, and troubleshooting capability. The Cisco MWTM provides the following key features:

- Event Monitoring
- Web-Based Reporting
- Autodiscovery and Topology
- Inventory
- OSS Integration
- Security
- Client/Server Architecture
- Multiple OS Support

The Cisco MWTM integrates with any SNMP-based monitoring system, such as Cisco Info Center products. In addition, the Cisco MWTM collects a large amount of performance data that can be exported or directly accessed from the database. This data can then be used by performance reporting applications. For more information about MWTM, see

[http://www.cisco.com/en/US/products/ps6472/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6472/tsd_products_support_series_home.html).

## Configuring SNMP Support

Use the following instructions to configure SNMP support: setting up the community access, establishing a message queue for each trap host, enabling the router to send SNMP traps, enabling SNMP traps for alarms, and enabling SNMP traps for a specific environment. You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.

**Note**

To view the current MIBs that the Cisco MWR 2941 supports, see the *Release Notes for Cisco MWR 2941 Mobile Wireless Edge Router for Cisco IOS Release 12.2(33)MRA*.

**Note**

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the **Router#** prompt.

To configure a Cisco MWR 2941 for SNMP, follow these steps while in the global configuration mode:

**Step 1**

To set up the community access string to permit access to the SNMP, use the **snmp-server community** command. The **no** form of this command removes the specified community string.

```
Router(config)# snmp-server community string [view view-name] [ro | rw] [number]
```

- *string*—Community string that acts like a password and permits access to the SNMP protocol.
- **view** *view-name*—(Optional) Name of a previously defined view. The view defines the objects available to the community.
- **ro**—(Optional) Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw**—(Optional) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.
- *number*—(Optional) Integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.

For example, the following command sets up the community access string as xxxxx with read-only access:

```
Router(config)# snmp-server community xxxxx RO
```

**Step 2**

To establish the message queue length for each trap host, use the **snmp-server queue-length** command.

```
Router(config)# snmp-server queue-length length
```

- *length*—Integer that specifies the number of trap events that can be held before the queue must be emptied.

For example, the following command establishes the number of trap events to 100:

```
Router(config)# snmp-server queue-length 100
```

**Step 3** To enable the router to send SNMP traps or informs (SNMP notifications), use the **snmp-server enable traps** command. Use the **no** form of this command to disable SNMP notifications.

```
Router(config)# snmp-server enable traps [notification-type] [notification-option]
```

- **notification-type—snmp [authentication]**—Enables RFC 1157 SNMP notifications. Note that use of the **authentication** keyword produces the same effect as not using the **authentication** keyword. Both the **snmp-server enable traps snmp** and **snmp-server enable traps snmp authentication** forms of this command will globally enable (or, if using the **no** form, disable) the following SNMP traps:
  - authentication failure
  - linkup
  - linkdown
  - coldstart
  - warmstart
- **notification-option**—(Optional) **atm pvc [interval seconds] [fail-interval seconds]**—The optional interval seconds keyword/argument combination specifies the minimum period between successive traps, in the range from 1 to 3600. Generation of PVC traps is dampened by the notification interval to prevent trap storms. No traps are sent until the interval lapses. The default interval is 30.  
The optional fail-interval seconds keyword/argument combination specifies the minimum period for storing the failed time stamp, in the range from 0 to 3600. The default fail-interval is 0.
- **envmon [voltage | shutdown | supply | fan | temperature]**—When the **envmon** keyword is used, you can enable a specific environmental notification type, or accept all notification types from the environmental monitor system. If no option is specified, all environmental notifications are enabled. The option can be one or more of the following keywords: **voltage**, **shutdown**, **supply**, **fan**, and **temperature**.
- **isdn [call-information | isdn u-interface]**—When the **isdn** keyword is used, you can specify the **call-information** keyword to enable an SNMP ISDN call information notification for the ISDN MIB subsystem, or you can specify the **isdnu-interface** keyword to enable an SNMP ISDN U interface notification for the ISDN U interface MIB subsystem.
- **repeater [health | reset]**—When the **repeater** keyword is used, you can specify the **repeater** option. If no option is specified, all repeater notifications are enabled. The option can be one or more of the following keywords:
  - **health**—Enables IETF Repeater Hub MIB (RFC 1516) health notification.
  - **reset**—Enables IETF Repeater Hub MIB (RFC 1516) reset notification.

For example, the following command enables traps for SNMP link down, link up, coldstart, and warmstart:

```
Router(config)# snmp-server enable traps snmp linkdown linkup coldstart warmstart
```

**Step 4** To enable SNMP traps for all IP-RAN notifications, enter:

```
Router(config)# snmp-server enable traps ipran
```

**Note**

Besides enabling SNMP traps for all IP-RAN notifications, you can also enable traps for IP-RAN GSM alarms, UMTS alarms, and general information about the backhaul utilization (see [Appendix B, “Cisco MWR 2941 Router Command Reference”](#) for descriptions on how to use these SNMP commands.

**Step 5** To enable SNMP traps for a specific environment, enter:

```
Router(config)# snmp-server enable traps envmon
```

**Step 6** To specify the recipient of an SNMP notification operation, use the **snmp-server host** command. To remove the specified host, use the **no** form of this command.

```
Router(config)# snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]] community-string [udp-port port] [notification-type]
```

- *host-addr*—Name or Internet address of the host (the targeted recipient).
- **traps**—(Optional) Send SNMP traps to this host. This is the default.
- **informs**—(Optional) Send SNMP informs to this host.
- **version**—(Optional) Version of the Simple Network Management Protocol (SNMP) used to send the traps. Version 3 is the most secure model, as it allows packet encryption with the **priv** keyword. If you use the version keyword, one of the following must be specified:
  - **1**—SNMPv1. This option is not available with informs.
  - **2c**—SNMPv2C.
  - **3**—SNMPv3. The following three optional keywords can follow the version 3 keyword:
    - **auth** (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication
    - **noauth** (Default). The noAuthNoPriv security level. This is the default if the [auth | noauth | priv] keyword choice is not specified.
    - **priv** (Optional). Enables Data Encryption Standard (DES) packet encryption (also called “privacy”).
- *community-string*—Password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command before using the **snmp-server host** command.
- **udp-port port**—UDP port of the host to use. The default is 162.
- *notification-type*—(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords:
  - **aaa\_server**—Enable SNMP AAA Server traps.
  - **atm**—Enable SNMP atm Server traps.
  - **ccme**—Enable SNMP ccme traps.
  - **cnpd**—Enable NBAR Protocol Discovery traps.
  - **config**—Enable SNMP config traps.
  - **config-copy**—Enable SNMP config-copy traps.
  - **cpu**—Allow cpu related traps.
  - **dial**—Enable SNMP dial control traps.

- **dnis**—Enable SNMP DNIS traps.
- **ds0-busyout**—Enable ds0-busyout traps.
- **ds1**—Enable SNMP DS1 traps.
- **ds1-loopback**—Enable ds1-loopback traps.
- **ds3**—Enable SNMP DS3 traps.
- **dsp**—Enable SNMP dsp traps.
- **eigrp**—Enable SNMP EIGRP traps.
- **entity**—Enable SNMP entity traps.
- **envmon**—Enable SNMP environmental monitor traps.
- **flash**—Enable SNMP FLASH notifications.
- **frame-relay**—Enable SNMP frame-relay traps.
- **hsrp**—Enable SNMP HSRP traps.
- **icsudsu**—Enable SNMP ICSUDSU traps.
- **ipmulticast**—Enable SNMP ipmulticast traps.
- **ipran**—Enable IP-RAN Backhaul traps.
- **ipsla**—Enable SNMP IP SLA traps.
- **isdn**—Enable SNMP isdn traps.
- **12tun**—Enable SNMP L2 tunnel protocol traps.
- **mpls**—Enable SNMP MPLS traps.
- **msdp**—Enable SNMP MSDP traps.
- **mvpn**—Enable Multicast Virtual Private Networks traps.
- **ospf**—Enable OSPF traps.
- **pim**—Enable SNMP PIM traps.
- **pppoe**—Enable SNMP pppoe traps.
- **pw**—Enable SNMP PW traps.
- **rsvp**—Enable RSVP flow change traps.
- **snmp**—Enable SNMP traps.
- **srst**—Enable SNMP srst traps.
- **syslog**—Enable SNMP syslog traps.
- **tty**—Enable TCP connection traps.
- **voice**—Enable SNMP voice traps.
- **vrrp**—Enable SNMP vrrp traps.
- **vtp**—Enable SNMP VTP traps.
- **xgcp**—Enable XGCP protocol traps.

For example, the following command specifies a recipient of the SNMP operation with a host-address of 10.20.30.40 with a version SNMP of SNMPv2C:

```
Router(config)# snmp-server host 10.20.30.40 version 2c
```

- Step 7** Exit the global configuration mode.

```
Router(config)# exit
```

---

## Enabling Remote Network Management

To enable remote network management of the Cisco MWR 2941, do the following:

- Step 1** At the privileged EXEC prompt, enter the following command to access the configuration mode:

```
Router# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#
```

- Step 2** At the configuration prompt, enter the following command to assign a host name to each of the network management workstations:

```
Router(config)# ip host hostname ip_address
```

Where *hostname* is the name assigned to the Operations and Maintenance (O&M) workstation and *ip\_address* is the address of the network management workstation.

- Step 3** Enter the following commands to create a loopback interface for O&M.

```
Router(config)# interface loopback number  
Router(config-if)# ip address ip_address subnet_mask
```



**Note** For more information, see the [“Configuring Gigabit Ethernet Interfaces”](#) section on page 4-4.

---

- Step 4** Exit interface configuration mode:

```
Router(config-if)# exit
```

- Step 5** At the configuration prompt, enter the following command to specify the recipient of a Simple Network Management Protocol (SNMP) notification operation:

```
Router(config)# snmp-server host hostname [traps | informs] [version {1 | 2c | 3 [auth |  
noauth | priv]}] community-string [udp-port port] [notification-type]
```

Where *hostname* is the name assigned to the Cisco Info Center workstation with the **ip host** command in [Step 2](#).



**Note** See the [“Configuring Multiprotocol Label Switching \(MPLS\)”](#) section on page 4-58 for more information about configuring Steps 5 through 8 in this procedure.

---

- Step 6** Enter the following commands to specify the public and private SNMP community names:

```
Router(config)# snmp-server community public RO  
Router(config)# snmp-server community private RW
```

- Step 7** Enter the following command to enable the sending of SNMP traps:

```
Router(config)# snmp-server enable traps
```

- Step 8** Enter the following command to specify the loopback interface from which SNMP traps should originate:

```
Router(config)# snmp-server trap-source loopback number
```

Where *number* is the number of the loopback interface you configured for the O&M in [Step 3](#).

- Step 9** At the configuration prompt, press **Ctrl-Z** to exit configuration mode.

- Step 10** Write the new configuration to nonvolatile memory as follows:

```
Router# copy running-config startup-config
```

## Show Commands for Monitoring the Cisco MWR 2941 Router

To monitor and maintain the Cisco MWR 2941 router, use the following commands:

| Command                                           | Purpose                                                                                                                                                                                                     |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show atm cell-packing</b>                      | Information about Layer 2 transport ATM cell-packing.                                                                                                                                                       |
| <b>show cem circuit</b>                           | Summary about the CEM circuit state, including controller, interface, and AC.<br><br>Also displays specific CEM circuit state, circuit parameters, and statistics/counters.                                 |
| <b>show cem platform</b>                          | CEM errors and information.                                                                                                                                                                                 |
| <b>show connection</b>                            | Displays the status of interworking connections.                                                                                                                                                            |
| <b>show controllers</b>                           | All network modules and their interfaces. Also displays the status of the VWIC relays when a VWIC is installed.                                                                                             |
| <b>show controllers gigabitethernet slot/port</b> | Information about initialization block, transmit ring, receive ring, and errors for the Fast Ethernet controller chip.                                                                                      |
| <b>show controllers e1</b>                        | Information about controller status specific to the controller hardware. Also displays statistics about the E1 link. If you specify a slot and a port number, statistics for each 15-minute period appears. |
| <b>show controllers t1</b>                        | Information about cable length, framing, firmware, and errors associated with the T1. With the Cisco MWR 2941 router, this command also shows the status of the relays on the VWIC.                         |
| <b>show dsl interface atm</b>                     | Displays information specific to the asymmetric digital subscriber line (ADSL) for a specified ATM interface.                                                                                               |
| <b>show gsm traffic</b>                           | Traffic rates in bits per second at 1 second, 5 seconds, 1 minute, 5 minutes, and 1 hour intervals for GSM data transmitted and received over the backhaul.                                                 |

| Command                                                | Purpose                                                                                                                               |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>show gsm-abis efficiency</b> [history]              | History of the GSM efficiency averages for compression/decompression at 1-second, 5-second, 1-minute, 5-minute, and 1-hour intervals. |
| <b>show gsm-abis errors</b>                            | Error statistics counters of the GSM for compression/decompression.                                                                   |
| <b>show gsm-abis packets</b>                           | Packet statistics counters of the GSM for compression/decompression.                                                                  |
| <b>show gsm-abis peering</b> [details]                 | Peering status, statistics, and history of the GSM compression/decompression.                                                         |
| <b>show interface</b> <i>type slot/port</i>            | Configuration and status of the specified interface.                                                                                  |
| <b>show interface switchport backup</b>                | Status information about the backup switchport.                                                                                       |
| <b>show interface virtual-cem</b> <i>slot/port</i>     | Status of the CEM interface.                                                                                                          |
| <b>show interface gigabitethernet</b> <i>slot/port</i> | Status of the FE interface.                                                                                                           |
| <b>show ip mroute</b>                                  | Contents of the multicast routing (mroute) table.<br><b>Note</b> Multicast routing applies only to PTP redundancy.                    |
| <b>show mpls l2transport vc</b>                        | Information about Any Transport over MPLS (AToM) virtual circuits (VCs) that are enabled to route Layer 2 packets on a router.        |
| <b>show network-clocks</b>                             | Network clocking configuration.                                                                                                       |
| <b>show platform hardware</b>                          | Status of hardware devices on the Cisco MWR 2941 router.                                                                              |
| <b>show policy-map</b>                                 | Configuration of all classes for a specified service policy map or of all classes for all existing policy maps.                       |
| <b>show policy-map interface</b>                       | Statistics and the configurations of the input and output policies that are attached to an interface.                                 |
| <b>show ppp multilink</b>                              | MLP and multilink bundle information.                                                                                                 |
| <b>show ppp multilink interface</b> <i>number</i>      | Multilink information for the specified interface.                                                                                    |
| <b>show protocols</b>                                  | Protocols configured for the router and the individual interfaces.                                                                    |
| <b>show ptp clock</b>                                  | Displays ptp clock information.                                                                                                       |
| <b>show ptp foreign-master-record</b>                  | Displays PTP foreign master records.                                                                                                  |
| <b>show ptp parent</b>                                 | Displays PTP parent properties.                                                                                                       |
| <b>show ptp port</b>                                   | Displays PTP port properties.                                                                                                         |
| <b>show ptp time-property</b>                          | Displays PTP clock time properties.                                                                                                   |
| <b>show xconnect all</b>                               | xconnect information.                                                                                                                 |



## Configuring Cisco Networking Services (CNS)

Cisco Networking Services (CNS) is a collection of services that can provide remote configuration of Cisco IOS networking devices and remote execution of some command-line interface (CLI) commands. CNS allows a Cisco MWR 2941 deployed and powered on in the field to automatically download its configuration.

**Note**

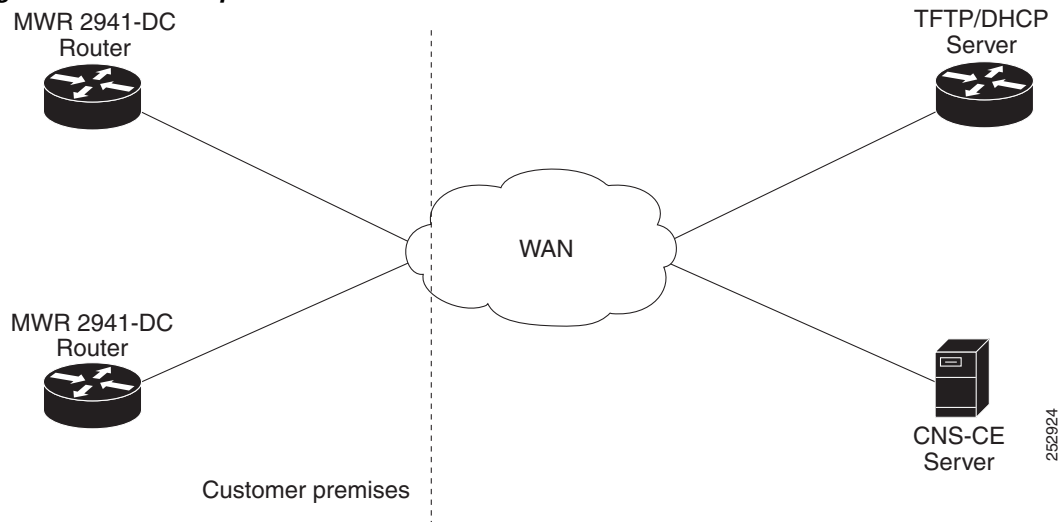
The Cisco MWR 2941 only supports CNS over motherboard Ethernet interfaces. Other interface types do not support CNS.

To enable CNS, you need the following items:

- A DHCP server (standalone or enabled on the carrier edge router)
- A TFTP server (standalone or enabled on the carrier edge router)
- A server running the Cisco Configuration Engine (formerly known as the CNS-CE server)

Figure 4-5 shows a sample CNS network.

**Figure 4-5 Sample CNS Network**

**Note**

These devices must be connected through onboard Ethernet interfaces. CNS connections over Ethernet HWICs and non-ethernet interfaces are not supported.

The following sections describe how to configure CNS on the Cisco MWR 2941.

- [Process Overview](#)
- [Configuring a DHCP Server](#)
- [Configuring a TFTP Server](#)
- [Configuring the Cisco Configuration Engine](#)
- [Verifying the Configuration](#)

## Process Overview

The following sections provide an overview of the steps that take place during a Cisco MWR 2941 zero-touch deployment and image download.

### Zero-Touch Deployment

The following sequence of events takes place when a CNS-enabled Cisco MWR 2941 boots and receives a configuration.

1. The Cisco MWR 2941 boots and sends a DHCP Discover message.
2. The DHCP Server replies with DHCP Offer.
3. The Cisco MWR 2941 sends DHCP Request.
4. The DHCP Server replies with option 150 for TFTP.
5. The Cisco MWR 2941 requests network-config file via TFTP.
6. The TFTP server sends the Cisco MWR 2941 a network-config file.
7. The Cisco MWR 2941 sends an HTTP request to the CNS-CE server.
8. The CNS-CE server sends a configuration template to the Cisco MWR 2941.
9. Successful event.
10. Publish success event.

### Image Download

The following events take place when a CNS-enabled Cisco MWR 2941 downloads a new image.

1. The CNS-CE server requests inventory (disk/flash info) from the Cisco MWR 2941-DC.
2. The Cisco MWR 2941-DC sends an inventory.
3. The CNS-CE server sends an image location.
4. The Cisco MWR 2941-DC sends an TFTP image request.
5. The Cisco MWR 2941-DC downloads an image from the TFTP server.
6. The Cisco MWR 2941-DC indicates that the image download is complete.
7. The CNS-CE server reboots the Cisco MWR 2941-DC router.

## Configuring a DHCP Server

The Cisco MWR 2941 requires a DHCP server for zero-touch deployment. The DHCP server is typically implemented on the carrier edge router. You can use the following sample configuration to enable a DHCP server on the edge router.

```
ip dhcp excluded-address 30.30.1.6
ip dhcp excluded-address 30.30.1.20 30.30.1.255
!
ip dhcp pool mwrdhcp
network 30.30.1.0 255.255.255.0
option 150 ip 30.30.1.6
! Specifies the TFTP server address
!
default-router 30.30.1.6
```

## Configuring a TFTP Server

You need to set up a TFTP server in order to provide a bootstrap image to 2941s when they boot.

### Creating a Bootstrap Configuration

The TFTP server should store a configuration that the Cisco MWR 2941 uses to boot. The following sample configuration specifies 30.30.1.20 as the CNS server IP address and port 80 for the configuration service.

```
hostname test-2941
!
cns trusted-server all-agents 30.30.1.20
cns event 30.30.1.20 11011 keepalive 60 3
cns config initial 30.30.1.20 80
cns config partial 30.30.1.20 80
cns id hostname
cns id hostname event
cns id hostname image
cns exec 80
logging buffered 20000
!
end
```

For more information about the commands used in this configuration, see [Appendix B](#), “Cisco MWR 2941 Router Command Reference” and the *Cisco Configuration Engine Installation & Configuration Guide*.

### Enabling a TFTP Server on the Edge Router

The Cisco MWR 2941 requires a TFTP server for zero-touch deployment. The TFTP server is typically implemented on the carrier edge router. You can use the following global configuration commands enable a TFTP server on the edge router that can send a configuration to the Cisco MWR 2941 router.

```
tftp-server sup-bootflash:network-config
tftp-server sup-bootflash:test-2941-config
```

Once the Cisco MWR 2941 boots with this configuration, it can connect to the CNS-CE server.

## Configuring the Cisco Configuration Engine

The Cisco Configuration Engine (formerly known as the Cisco CNS Configuration Engine) allows you to remotely manage configurations and IOS software images on Cisco devices including the Cisco MWR 2941.

Once the Cisco MWR 2941 downloads the bootstrap configuration and connects to the Cisco Configuration Engine server, you can use the server to download a full configuration to the router. You can also use the CNS-CE server to complete any of the following tasks:

- Manage configuration templates—The CNS-CE server can store and manage configuration templates.
- Download a new image—You can use the CNS-CE server to load a new IOS image on a Cisco MWR 2941 router.
- Loading a new config—You can use the CNS-CE server to load a new configuration file on a Cisco MWR 2941 router.

- Enable identification—You can use a unique CNS agent ID to verify the identity of a host device prior to communication with the CNS-CE server.
- Enable Authentication—You can configure the CNS-CE server to require a unique password from the 2941 router as part of any communication handshake.
- Enable encryption—You can enable Secure Socket Layer (SSL) encryption for the HTTP sessions between the CNS agent devices (Cisco MWR 2941 routers) and the CNS-CE server.

For instructions about how to use the CNS-CE server, see the [Cisco Configuration Engine Installation & Configuration Guide](#).

## Verifying the Configuration

You can use the following IOS commands to verify the CNS configuration on the Cisco MWR 2941.

- **show cns event connection**
- **show cns image connection**
- **show cns image inventory**
- **debug cns all**



# APPENDIX **A**

## Sample Configurations

---

The Cisco MWR 2941 supports a variety of topology designs based on various GSM configurations, including the following common topologies:

- A *backhaul* interface is used to transfer GSM traffic. The traditional backhaul interface is comprised of one or more T1/E1 controllers logically combined to form a *multilink* connect (except HSDPA, which uses the backhaul interface for T1/E1 line clocking).
- A *shorthaul* interface is used to transfer GSM traffic from the BTS/Node-B to the Cisco MWR 2941 router and from the Cisco MWR 2941 router to the BSC/RNC. The traditional shorthaul connections on the RAN devices are connected through the Cisco T1 or E1 interface card.
- Topology naming conventions such as 3x2 and 4x3 are used to describe the type of deployment. The first number signifies the number of GSM shorthaul interface connections and the second number signifies the number of multilink backhaul interface connections.

## Sample Configurations

This appendix includes examples of the following real-world configurations for the Cisco MWR 2941:

- [Pseudowire Configurations, page A-2](#)
- [GRE Tunneling Configurations, page A-26](#)
- [Routing Sample Configurations, page A-27](#)
- [Multicast Sample Configurations, page A-37](#)
- [PTP Sample Configurations, page A-38](#)
- [Layer 3 VPN Sample Configuration, page A-46](#)
- [QoS Sample Configurations, page A-48](#)
- [Resilient Ethernet Protocol \(REP\) Sample Configuration, page A-51](#)
- [Cisco Networking Services \(CNS\) Zero Touch Deployment Configuration, page A-54](#)
- [CFM and ELMI Sample Configuration, page A-54](#)



### Note

The network addresses in these examples are generic addresses, so you must replace them with actual addresses for your network.

## Pseudowire Configurations

The following sections contain configuration examples for pseudowire connections.

- [Asymmetric Pseudowire Configuration](#)
- [Pseudowire Redundancy Configuration](#)
- [TDM over MPLS Configuration](#)
- [ATM over MPLS Configuration](#)
- [Ethernet over MPLS Configuration](#)



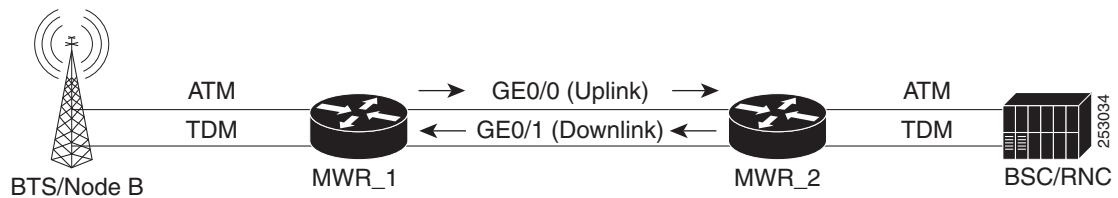
### Note

When creating IP routes with a pseudowire configuration, we recommend that you build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as `ip route 1.1.1.1 255.255.255.255 1.2.3.4`. For more information about configuring pseudowire, see [Configuring Pseudowire](#), page 4-73.

## Asymmetric Pseudowire Configuration

The following example shows an asymmetric PWE3 configuration ([Figure A-1](#)).

**Figure A-1 Asymmetric Pseudowire Configuration**



### MWR\_1

```

version 12.4
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime

!
hostname MWR1
!
boot-start-marker
boot-end-marker
!
card type e1 0 0
card type e1 0 1
!
!
ip cef
!
!
controller E1 0/0
  clock source internal
  cem-group 1 unframed
!
controller E1 0/1
  clock source internal

```

```
cem-group 20 unframed
!
controller E1 0/2
clock source internal
cem-group 12 unframed
!
controller E1 0/3
clock source internal
cem-group 30 unframed
!
controller E1 0/4
clock source internal
cem-group 8 unframed
!
controller E1 0/5
clock source internal
cem-group 25 unframed
!
controller E1 1/0
mode atm
clock source internal
!
controller E1 1/1
mode atm
clock source internal
!
controller E1 1/2
mode atm
clock source internal
!
controller E1 1/3
!
!
pseudowire-class mpls
encapsulation mpls
preferred-path peer 50.0.0.2
!
!
interface Loopback50
ip address 50.0.0.1 255.255.255.255
!
interface CEM0/0
no ip address
cem 1
xconnect 50.0.0.2 1 encapsulation mpls
!
!
interface Vlan 20
ip address 20.0.0.1 255.0.0.0
mpls ip
!
interface CEM0/1
no ip address
cem 20
xconnect 50.0.0.2 2 encapsulation mpls
!
interface Vlan 60
ip address 60.0.0.1 255.0.0.0
mpls ip
!
interface CEM0/2
no ip address
cem 12
xconnect 50.0.0.2 3 encapsulation mpls
```

```
!  
!  
interface CEM0/3  
  no ip address  
  cem 30  
  xconnect 50.0.0.2 4 encapsulation mpls  
!  
interface CEM0/4  
  no ip address  
  cem 8  
  xconnect 50.0.0.2 5 encapsulation mpls  
!  
!  
interface CEM0/5  
  no ip address  
  cem 25  
  xconnect 50.0.0.2 6 encapsulation mpls  
!  
interface GigabitEthernet0/0  
  switchport access vlan 20  
  duplex auto  
  speed auto  
!  
interface GigabitEthernet0/1  
  switchport access vlan 60  
  duplex auto  
  speed auto  
!  
interface ATM1/0  
  no ip address  
  load-interval 30  
  scrambling-payload  
  mcpt-timers 1000 5000 10000  
  no ilmi-keepalive  
  pvc 0/5 l2transport  
    encapsulation aal0  
    cell-packing 10 mcpt-timer 3  
    xconnect 50.0.0.2 10 pw-class mpls  
!  
  pvc 0/6 l2transport  
    xconnect 50.0.0.2 20 pw-class mpls  
!  
  pvc 0/7 l2transport  
    encapsulation aal0  
    cell-packing 28 mcpt-timer 3  
    xconnect 50.0.0.2 30 encapsulation mpls pw-class mpls one-to-one  
!  
  pvc 0/8 l2transport  
    xconnect 50.0.0.2 40 pw-class mpls  
!  
  pvc 0/9 l2transport  
    encapsulation aal0  
    xconnect 50.0.0.2 50 pw-class mpls one-to-one  
!  
!  
interface ATM1/0.1 point-to-point  
  pvc 0/15 l2transport  
    xconnect 50.0.0.2 13 pw-class mpls  
!  
interface ATM1/0.2 multipoint  
  cell-packing 2 mcpt-timer 1  
  xconnect 50.0.0.2 12 encapsulation mpls  
  pvc 0/10 l2transport  
    encapsulation aal0
```



```
!
pvc 0/11 l2transport
 encapsulation aal0
!
pvc 0/12 l2transport
 encapsulation aal0
!
pvc 0/13 l2transport
 encapsulation aal0
!
!
interface ATM1/0.3 point-to-point
pvc 0/16 l2transport
 encapsulation aal0
 xconnect 50.0.0.2 14 encapsulation mpls
!
!
interface ATM1/0.4 point-to-point
pvc 0/17 l2transport
 encapsulation aal0
 xconnect 50.0.0.2 15 pw-class mpls one-to-one
!
!
interface ATM1/0.6 multipoint
pvc 0/26 l2transport
 xconnect 50.0.0.2 16 pw-class mpls
!
pvc 0/27 l2transport
 encapsulation aal0
 cell-packing 8 mcpt-timer 3
 xconnect 50.0.0.2 17 pw-class mpls
!
pvc 0/28 l2transport
 encapsulation aal0
 cell-packing 16 mcpt-timer 2
 xconnect 50.0.0.2 18 pw-class mpls
!
!
interface ATM1/0.7 multipoint
!
interface ATM1/1
 no ip address
 scrambling-payload
 mcpt-timers 1000 5000 10000
 no ilmi-keepalive
 cell-packing 20 mcpt-timer 2
 xconnect 50.0.0.2 11 encapsulation mpls
pvc 0/21 l2transport
 encapsulation aal0
!
pvc 0/22 l2transport
 encapsulation aal0
!
pvc 0/23 l2transport
 encapsulation aal0
!
!
interface ATM1/1.1 point-to-point
!
interface ATM1/1.2 multipoint
!
interface ATM1/2
 no ip address
 scrambling-payload
```

```

    ima-group 0
    no ilmi-keepalive
    !
ip route 50.0.0.2 255.255.255.255 20.0.0.2
!
ip http server
no ip http secure-server
!
!
mpls ldp router-id Loopback50 force
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  login
!
network-clock-select 1 BITS
!
end

```

## MWR\_2

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname MWR2
!
boot-start-marker
boot-end-marker
!
card type e1 0 0
card type e1 0 1
!
enable password mypassword
!
no aaa new-model
!
ip cef
!
!
controller E1 0/0
  cem-group 1 unframed
!
controller E1 0/1
  cem-group 20 unframed
!
controller E1 0/2
  cem-group 12 unframed
!
controller E1 0/3
  cem-group 30 unframed
!
controller E1 0/4
  cem-group 8 unframed
!
controller E1 0/5
  cem-group 25 unframed
!
controller E1 1/0
  mode atm

```

```
clock source internal
!
controller E1 1/1
mode atm
clock source internal
!
controller E1 1/2
mode atm
clock source internal
!
controller E1 1/3
clock source internal
!
pseudowire-class mpls
encapsulation mpls
preferred-path peer 50.0.0.1
!
!
interface Loopback50
ip address 50.0.0.2 255.255.255.255
!
interface CEM0/0
no ip address
cem 1
xconnect 50.0.0.1 1 encapsulation mpls
!
!
interface Vlan20
ip address 20.0.0.2 255.0.0.0
mpls ip
!
interface Vlan60
ip address 60.0.0.2 255.0.0.0
mpls ip
!
interface GigabitEthernet0/0
switchport access vlan 20
duplex auto
speed auto
!
interface GigabitEthernet0/1
switchport access vlan 60
duplex auto
speed auto
!
!
interface CEM0/1
no ip address
cem 20
xconnect 50.0.0.1 2 encapsulation mpls
!
!
interface CEM0/2
no ip address
cem 12
xconnect 50.0.0.1 3 encapsulation mpls
!
!
interface CEM0/3
no ip address
cem 30
xconnect 50.0.0.1 4 encapsulation mpls
!
!
```

```
interface CEM0/4
no ip address
cem 8
xconnect 50.0.0.1 5 encapsulation mpls
!
!
interface CEM0/5
no ip address
cem 25
xconnect 50.0.0.1 6 encapsulation mpls
!
!
interface ATM1/0
ip address 1.1.1.2 255.0.0.0
load-interval 30
scrambling-payload
mcpt-timers 1000 5000 10000
no ilmi-keepalive
pvc 0/5 l2transport
encapsulation aal0
cell-packing 25 mcpt-timer 3
xconnect 50.0.0.1 10 pw-class mpls
!
pvc 0/6 l2transport
xconnect 50.0.0.1 20 pw-class mpls
!
pvc 0/7 l2transport
encapsulation aal0
cell-packing 12 mcpt-timer 2
xconnect 50.0.0.1 30 encapsulation mpls pw-class mpls one-to-one
!
pvc 0/8 l2transport
xconnect 50.0.0.1 40 pw-class mpls
!
pvc 0/9 l2transport
encapsulation aal0
xconnect 50.0.0.1 50 pw-class mpls one-to-one
!
pvc 0/99
protocol ip 1.1.1.1 broadcast
encapsulation aal5snap
!
!
interface ATM1/0.1 point-to-point
pvc 0/15 l2transport
xconnect 50.0.0.1 13 pw-class mpls
!
!
interface ATM1/0.2 multipoint
cell-packing 10 mcpt-timer 2
xconnect 50.0.0.1 12 encapsulation mpls
pvc 0/10 l2transport
encapsulation aal0
!
pvc 0/11 l2transport
encapsulation aal0
!
pvc 0/12 l2transport
encapsulation aal0
!
pvc 0/13 l2transport
encapsulation aal0
!
!
```

```
interface ATM1/0.3 point-to-point
 pvc 0/16 l2transport
  encapsulation aal0
  xconnect 50.0.0.1 14 encapsulation mpls
 !
!
interface ATM1/0.4 point-to-point
 pvc 0/17 l2transport
  encapsulation aal0
  xconnect 50.0.0.1 15 pw-class mpls one-to-one
 !
!
interface ATM1/0.6 multipoint
 pvc 0/26 l2transport
  xconnect 50.0.0.1 16 pw-class mpls
 !
 pvc 0/27 l2transport
  encapsulation aal0
  cell-packing 18 mcpt-timer 3
  xconnect 50.0.0.1 17 pw-class mpls
 !
 pvc 0/28 l2transport
  encapsulation aal0
  cell-packing 24 mcpt-timer 2
  xconnect 50.0.0.1 18 pw-class mpls
 !
!
interface ATM1/0.7 multipoint
!
interface ATM1/1
 no ip address
 scrambling-payload
  mcpt-timers 1000 5000 10000
 no ilmi-keepalive
  cell-packing 20 mcpt-timer 2
 xconnect 50.0.0.1 11 encapsulation mpls
 pvc 0/21 l2transport
  encapsulation aal0
 !
 pvc 0/22 l2transport
  encapsulation aal0
 !
 pvc 0/23 l2transport
  encapsulation aal0
 !
!
interface ATM1/2
 no ip address
 scrambling-payload
 ima-group 0
 no ilmi-keepalive
!
ip route 50.0.0.1 255.255.255.255 60.0.0.1
!
!
ip http server
no ip http secure-server
!
!
mpls ldp router-id Loopback50 force
!
!
!
line con 0
```

```

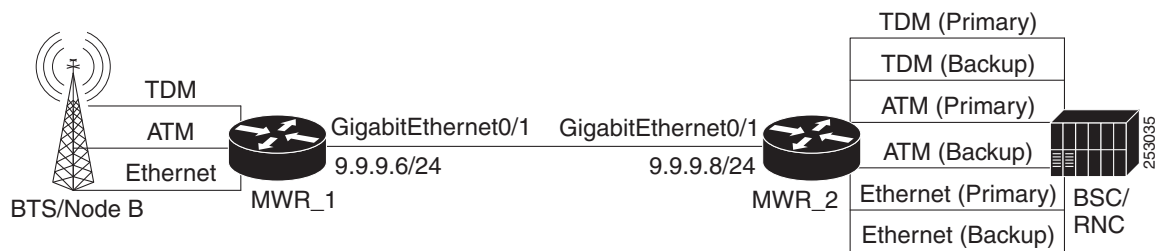
exec-timeout 0 0
line aux 0
line vty 0 4
  exec-timeout 0 0
  login
!
network-clock-select 1 BITS
!
end

```

## Pseudowire Redundancy Configuration

The following example shows a pseudowire redundancy configuration (Figure A-2).

**Figure A-2 Pseudowire3 Redundancy Configuration**



### MWR\_1

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname mwr-1
!
boot-start-marker
boot-end-marker
!
card type e1 0 1
card type e1 0 2
!
ip cef
!
controller E1 0/0
  clock source internal
  cem-group 0 unframed
!
controller E1 0/1
!
controller E1 0/2
!
controller E1 0/3
  clock source internal
!
controller E1 1/0
  mode atm
  clock source internal
!
controller E1 1/1
!
controller E1 1/2
!

```

```
controller E1 1/3
  clock source internal
!
interface CEM0/0
  cem 0
  xconnect 2.2.2.2 1 encapsulation mpls
  backup peer 2.2.2.2 2
  backup delay 20 20
!
interface ATM1/0
  no ip address
  scrambling-payload
  no ilmi-keepalive
  pvc 0/1 l2transport
    encapsulation aal0
  xconnect 2.2.2.2 3 encapsulation mpls
  backup peer 2.2.2.2 4
  backup delay 20 20
!
interface Loopback0
  no ip address
!
interface Loopback1
  ip address 1.1.1.1 255.255.255.255
  load-interval 30
!
interface Loopback101
  no ip address
!
!
interface Vlan 9
  ip address 9.9.9.6 255.255.255.0
  mpls ip
!
interface Vlan 10
  no ip address
  no ptp enable
  xconnect 2.2.2.2 10 encapsulation mpls
  backup peer 2.2.2.2 20
!
interface GigabitEthernet0/1
  switchport access vlan 9
  duplex auto
  speed auto
!
interface GigabitEthernet0/2
  switchport access vlan 10
  duplex auto
  speed auto
!
!
ip forward-protocol nd
ip route 2.2.2.2 255.255.255.255 9.9.9.8
!

!
control-plane
!
!
line con 0
  exec-timeout 0 0
  logging synchronous
line aux 0
line vty 0 4
```

```

exec-timeout 0 0
password mypassword
login
!
exception data-corruption buffer truncate
!
end

```

## MWR\_2

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname mwr-pe2
!
boot-start-marker
boot-end-marker
!
card type e1 0 0
card type e1 0 1
card type e1 0 2
!
!
ip cef
!
!
controller E1 0/0
cem-group 0 unframed
!
controller E1 0/1
clock source internal
cem-group 0 unframed
!
controller E1 0/2
!
controller E1 0/3
clock source internal
!
controller E1 0/4
clock source internal
!
controller E1 0/5
!
controller E1 1/0
mode atm
clock source internal
!
controller E1 1/1
clock source internal
!
controller E1 1/2
clock source internal
!
controller E1 1/3
mode atm
clock source internal
!
! Primary
interface CEM0/0
cem 0
xconnect 1.1.1.1 1 encapsulation mpls
!

```



```
! Backup
interface CEM0/1
cem 0
  xconnect 1.1.1.1 2 encapsulation mpls
!
! Primary
interface ATM1/0
  no ip address
  scrambling-payload
  no ilmi-keepalive
pvc 0/1 l2transport
  encapsulation aal0
  xconnect 1.1.1.1 3 encapsulation mpls
!
! Backup
interface ATM1/3
  no ip address
  scrambling-payload
  no ilmi-keepalive
pvc 0/1 l2transport
  encapsulation aal0
  xconnect 1.1.1.1 4 encapsulation mpls
!
!
interface Loopback1
  ip address 2.2.2.2 255.255.255.255
!
!
interface Vlan 9
  ip address 9.9.9.8 255.255.255.0
  mpls ip
!
interface Vlan 10
  no ip address
  no ptp enable
  xconnect 1.1.1.1 10 encapsulation mpls
!
interface Vlan 20
  no ip address
  no ptp enable
  xconnect 1.1.1.1 20 encapsulation mpls
!
interface GigabitEthernet0/1
  switchport access vlan 9
  duplex auto
  speed auto
!
interface GigabitEthernet0/2
  switchport access vlan 10
  duplex auto
  speed auto
!
interface GigabitEthernet0/3
  switchport access vlan 20
  duplex auto
  speed auto
!
!
ip forward-protocol nd
ip route 1.1.1.1 255.255.255.255 9.9.9.6
!
!
mpls ldp router-id Loopback1 force
!
```

```

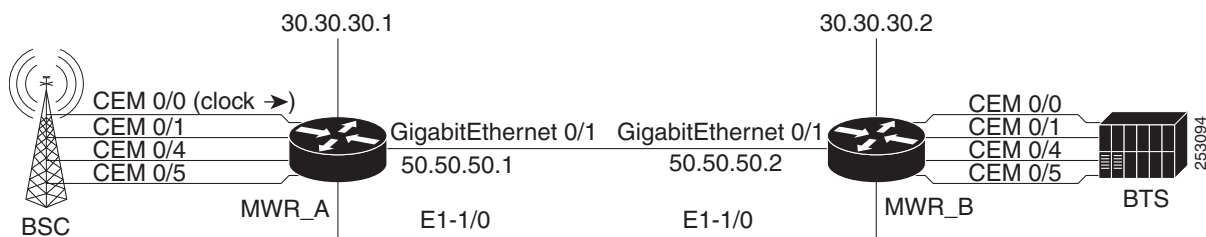
control-plane
!
no call rsvp-sync
!
!
!
line con 0
  exec-timeout 0 0
  logging synchronous
line aux 0
line vty 0 4
  exec-timeout 0 0
  password mypassword
  login
!
exception data-corruption buffer truncate
!
end

```

## TDM over MPLS Configuration

The following example shows a TDM over MPLS configuration that uses both SAToP and CESoPSN for E1 and T1. (Figure A-3)

**Figure A-3** TDM over MPLS Configuration



### MWR\_A

```

!
version 12.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname mwr_A
!
boot-start-marker
boot-end-marker
!
card type e1 0 0
card type e1 0 1
enable password xxx
!
no aaa new-model
clock timezone est -5
!
ip cef
!
controller E1 0/0
cem-group 0 timeslots 1-31
description E1 CESoPSN example

```

```
!  
controller E1 0/1  
clock source internal  
cem-group 1 unframed  
description E1 SATOP example  
!  
controller E1 0/4  
clock source internal  
cem-group 4 unframed  
description E1 SATOP example  
!  
controller E1 0/5  
clock source internal  
cem-group 5 timeslots 1-24  
description E1 CESoPSN example  
!  
controller E1 1/0  
clock source internal  
!  
controller E1 1/1  
!  
interface Loopback0  
ip address 30.30.30.1 255.255.255.255  
!  
interface GigabitEthernet0/1  
ip address 50.50.50.1 255.255.255.0  
mpls ip  
!  
interface CEM0/0  
no ip address  
cem 0  
    xconnect 30.30.30.2 300 encapsulation mpls  
!  
interface CEM0/1  
no ip address  
cem 1  
    xconnect 30.30.30.2 301 encapsulation mpls  
!  
!  
interface CEM0/4  
no ip address  
cem 4  
    xconnect 30.30.30.2 304 encapsulation mpls  
!  
!  
interface CEM0/5  
no ip address  
cem 5  
    xconnect 30.30.30.2 305 encapsulation mpls  
!  
!  
no ip classless  
ip route 30.30.30.2 255.255.255.255 50.50.50.2  
!  
no ip http server  
no ip http secure-server  
!  
line con 0  
password xxx  
login  
line aux 0  
password xxx  
login  
no exec
```

```
line vty 0 4
password xxx
login
!
network-clock-select 1 BITS
end
```

## MWR\_B

```
!
version 12.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname mwr_B
!
boot-start-marker
boot-end-marker
!
card type e1 0 0
card type e1 0 1
enable password xxx
!
no aaa new-model
clock timezone est -5
!
ip cef
!
controller E1 0/0
clock source internal
cem-group 0 timeslots 1-31
description E1 CESoPSN example
!
controller E1 0/1
clock source internal
cem-group 1 unframed
description E1 SATOP example
!
controller E1 0/4
clock source internal
cem-group 4 unframed
description T1 SATOP example
!
controller E1 0/5
clock source internal
cem-group 5 timeslots 1-24
description T1 CESoPSN example
!
controller E1 1/0

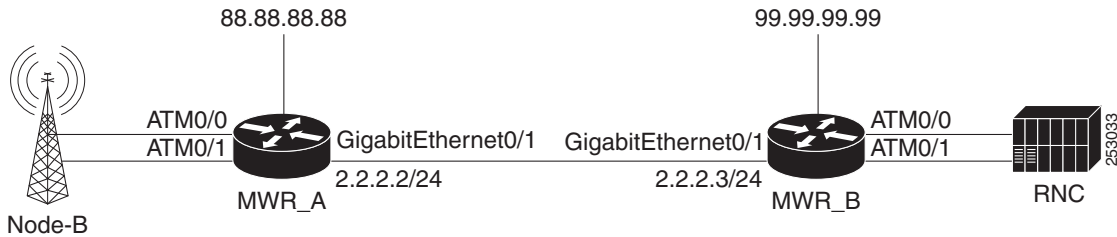
!
controller E1 1/1
!
interface Loopback0
ip address 30.30.30.2 255.255.255.255
!
!
interface GigabitEthernet0/1
ip address 50.50.50.2 255.255.255.0
mpls ip
!
interface CEM0/0
```

```
no ip address
cem 0
  xconnect 30.30.30.1 300 encapsulation mpls
!
interface CEM0/1
no ip address
cem 1
  xconnect 30.30.30.1 301 encapsulation mpls
!
interface CEM0/4
no ip address
cem 4
  xconnect 30.30.30.1 304 encapsulation mpls
!
!
interface CEM0/5
no ip address
cem 5
  xconnect 30.30.30.1 305 encapsulation mpls
!
!
no ip classless
ip route 30.30.30.1 255.255.255.255 50.50.50.1
!
no ip http server
no ip http secure-server
!
line con 0
password xxx
login
line aux 0
password xxx
login
no exec
line vty 0 4
password xxx
login
!
network-clock-select 1 E1 1/0
end
```

## ATM over MPLS Configuration

This example shows how to accomplish the following configurations ([Figure A-4](#)):

- AAL5 SDU mode PW on 0/1 PVC 0/100
- N:1 VCC cell mode PW on 0/1 PVC 0/101
- Multiple PVCs N:1 VCC cell mode PW on 0/1.1
- 1:1 VCC cell mode PW on 0/1 PVC 0/102
- Cell-packing for port mode PWs
- VCC cell-relay mode PWs
- PVC mapping for 0/1.1 N:1 VCC cell relay PWs

**Figure A-4 ATM over MPLS Configuration****MWR\_A**

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname mwr_A
!
boot-start-marker
boot-end-marker
!
card type e1 0 0
card type e1 0 1
logging buffered 4096
enable password mypassword
!
!
ip cef
!
!
no ip domain lookup
!
!
controller E1 0/0
mode atm
clock source internal
!
controller E1 0/1
mode atm
clock source internal
!
controller E1 0/2
mode atm
clock source internal
!
controller E1 0/3
mode atm
clock source internal
!
controller E1 0/4
!
controller E1 0/5
!
controller E1 1/0
!
controller E1 1/1
!
pseudowire-class mpls-exp-5
encapsulation mpls
mpls experimental 5

```

```
!  
!  
interface Loopback0  
  ip address 88.88.88.88 255.255.255.255  
!  
interface ATM0/0  
  no ip address  
  scrambling-payload  
  mcpt-timers 1000 2000 3000  
  no ilmi-keepalive  
  cell-packing 28 mcpt-timer 3  
  xconnect 99.99.99.99 100 encapsulation mpls  
  pvc 1/35 l2transport  
    encapsulation aal0  
  !  
  pvc 1/36 l2transport  
    encapsulation aal0  
  !  
  pvc 1/37 l2transport  
    encapsulation aal0  
  !  
interface GigabitEthernet0/0  
!  
interface ATM0/1  
  no ip address  
  load-interval 30  
  scrambling-payload  
  mcpt-timers 1000 2000 3000  
  no ilmi-keepalive  
  pvc 0/10  
  !  
  pvc 0/100 l2transport  
    encapsulation aal5  
    xconnect 99.99.99.99 1100 encapsulation mpls  
  !  
  pvc 0/101 l2transport  
    encapsulation aal0  
    cell-packing 28 mcpt-timer 3  
    xconnect 99.99.99.99 1101 encapsulation mpls  
  !  
  pvc 0/102 l2transport  
    encapsulation aal0  
    cell-packing 28 mcpt-timer 3  
    xconnect 99.99.99.99 1102 encapsulation mpls  
  !  
  pvc 0/103 l2transport  
    encapsulation aal0  
    cell-packing 28 mcpt-timer 3  
    xconnect 99.99.99.99 1103 pw-class mpls-exp-5  
  !  
  !  
interface ATM0/1.1 multipoint  
  cell-packing 28 mcpt-timer 3  
  xconnect 99.99.99.99 1200 encapsulation mpls  
  pvc 1/35 l2transport  
    encapsulation aal0  
    pw-pvc 2/135  
  !  
  pvc 1/36 l2transport  
    encapsulation aal0  
    pw-pvc 2/136  
  !  
  pvc 1/37 l2transport  
    encapsulation aal0
```

```

    pw-pvc 2/137
    !
    !
interface GigabitEthernet0/1
    description interface to 7600 fas 3/5
    ip address 2.2.2.2 255.255.255.0
    duplex auto
    speed auto
    mpls ip
    no keepalive
    !
interface ATM0/2
    no ip address
    scrambling-payload
    no ilmi-keepalive
    !
interface ATM0/3
    no ip address
    scrambling-payload
    no ilmi-keepalive
    !
ip route 99.99.99.99 255.255.255.255 2.2.2.3
    !
    !
ip http server
no ip http secure-server
    !
    !
mpls ldp router-id Loopback0
    !
    !
line con 0
    exec-timeout 0 0
line aux 0
line vty 0 4
    exec-timeout 0 0
    privilege level 15
    password mypassword
    login
    !
network-clock-select 1 E1 1/0
    !
end

```

## MWR\_B

```

    !
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
    !
hostname mwr_B
    !
boot-start-marker
boot-end-marker
    !
card type e1 0 0
card type e1 0 1
logging buffered 4096
enable password mypassword
    !
    !
ip cef
    !

```



```
!  
no ip domain lookup  
!  
!  
controller E1 0/0  
    mode atm  
!  
controller E1 0/1  
    mode atm  
!  
controller E1 0/2  
    mode atm  
!  
controller E1 0/3  
    mode atm  
!  
controller E1 0/4  
!  
controller E1 0/5  
!  
pseudowire-class mpls-exp-5  
    encapsulation mpls  
    mpls experimental 5  
!  
!  
interface Loopback0  
    ip address 99.99.99.99 255.255.255.255  
!  
interface ATM0/0  
    no ip address  
    scrambling-payload  
    mcpt-timers 1000 2000 3000  
    no ilmi-keepalive  
    cell-packing 28 mcpt-timer 3  
    xconnect 88.88.88.88 100 encapsulation mpls  
    pvc 1/35 l2transport  
        encapsulation aal0  
    !  
    pvc 1/36 l2transport  
        encapsulation aal0  
    !  
    pvc 1/37 l2transport  
        encapsulation aal0  
    !  
!  
interface GigabitEthernet0/0  
!  
interface ATM0/1  
    no ip address  
    scrambling-payload  
    mcpt-timers 1000 2000 3000  
    no ilmi-keepalive  
    pvc 0/2  
    !  
    pvc 0/100 l2transport  
        encapsulation aal5  
        xconnect 88.88.88.88 1100 encapsulation mpls  
    !  
    pvc 0/101 l2transport  
        encapsulation aal0  
        cell-packing 28 mcpt-timer 3  
        xconnect 88.88.88.88 1101 encapsulation mpls  
    !  
    pvc 0/102 l2transport
```

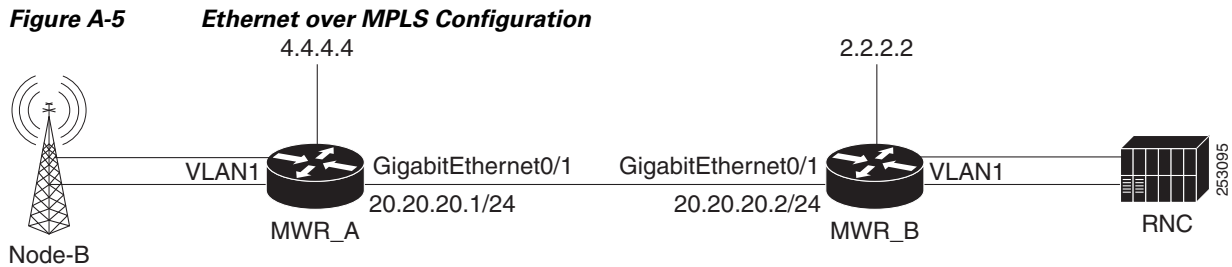
```

encapsulation aal0
cell-packing 28 mcpt-timer 3
xconnect 88.88.88.88 1102 encapsulation mpls
!
pvc 0/103 l2transport
encapsulation aal0
cell-packing 28 mcpt-timer 3
xconnect 88.88.88.88 1103 pw-class mpls-exp-5
!
interface ATM0/1.1 multipoint
cell-packing 28 mcpt-timer 3
xconnect 88.88.88.88 1200 encapsulation mpls
pvc 2/135 l2transport
encapsulation aal0
!
pvc 2/136 l2transport
encapsulation aal0
!
pvc 2/137 l2transport
encapsulation aal0
!
!
interface GigabitEthernet0/1
ip address 2.2.2.3 255.255.255.0
duplex auto
speed auto
mpls ip
!
interface ATM0/2
no ip address
scrambling-payload
ima-group 0
no ilmi-keepalive
!
interface ATM0/3
no ip address
scrambling-payload
ima-group 0
no ilmi-keepalive
!
ip route 88.88.88.88 255.255.255.255 2.2.2.2
!
!
ip http server
no ip http secure-server
!
!
mpls ldp router-id Loopback0
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
exec-timeout 0 0
password mypassword
login
!
network-clock-select 1 E1 0/0
!
end

```

## Ethernet over MPLS Configuration

The following configuration example shows an Ethernet pseudowire (aka EoMPLS) configuration. (Figure A-5)



### MWR\_A

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname mwr_A
!
boot-start-marker
boot-end-marker
!
card type e1 0 0
card type e1 0 1
logging buffered 4096
enable password mypassword
!
no aaa new-model
!
network-clock-select 1 E1 0/0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip cef
!
no ip domain lookup
ip domain name cisco.com
multilink bundle-name authenticated
mpls label protocol ldp
vpdn enable
!
!
controller E1 0/0
mode aim 1
!
controller E1 0/1
mode aim 1
!
controller E1 0/2
mode aim 1
!
controller E1 0/3
```

```
mode aim 1
!
controller E1 0/4
!
controller E1 0/5
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
!
interface GigabitEthernet0/4
 switchport trunk allowed vlan 1,2,20,1002-1005
 switchport mode trunk
!
interface GigabitEthernet0/5
 switchport trunk allowed vlan 1,2,40,1002-1005
 switchport mode trunk
!
interface Vlan20
 ip address 20.20.20.1 255.255.255.0
 no ptp enable
 mpls ip
!
interface Vlan40
 no ip address
 no ptp enable
 xconnect 2.2.2.2 10 encapsulation mpls
!
ip route 2.2.2.2 255.255.255.255 20.20.20.2
!
no ip http server
no ip http secure-server
!
!
mpls ldp router-id Loopback0
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password mypassword
 login
!
end
```

## MWR\_B

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname mwr_B
!
boot-start-marker
boot-end-marker
!
card type e1 0 0
card type e1 0 1
logging buffered 4096
```

```
enable password mypassword
!
no aaa new-model
!
network-clock-select 1 E1 0/0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip cef
!
no ip domain lookup
ip domain name cisco.com
multilink bundle-name authenticated
mpls label protocol ldp
vpdn enable
!
!
controller E1 0/0
mode aim 1
!
controller E1 0/1
mode aim 1
!
controller E1 0/2
mode aim 1
!
controller E1 0/3
mode aim 1
!
controller E1 0/4
!
controller E1 0/5
!
interface Loopback0
ip address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet0/4
switchport trunk allowed vlan 1,2,20,1002-1005
switchport mode trunk
!
interface GigabitEthernet0/5
switchport trunk allowed vlan 1,2,40,1002-1005
switchport mode trunk
!
interface Vlan20
ip address 20.20.20.2 255.255.255.0
no ptp enable
mpls ip
!
interface Vlan40
no ip address
no ptp enable
xconnect 4.4.4.4 10 encapsulation mpls
!
ip route 4.4.4.4 255.255.255.255 20.20.20.1
!
no ip http server
no ip http secure-server
!
!
mpls ldp router-id Loopback0
!
!
```

```
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  exec-timeout 0 0
  password mypassword
  login
!
end
```

## GRE Tunneling Configurations

The following configurations create pseudowire connections that use GRE tunnels:

- [CESoPSN with GRE Tunnel Backhaul](#)
- [ATM over MPLS AAL5 SDU Mode with GRE Backhaul](#)

For more information about how to configure GRE, see [Configuring GRE Tunneling, page 4-76](#).

**Note**

---

This section provides partial configurations intended to demonstrate a specific feature.

---

### CESoPSN with GRE Tunnel Backhaul

```
!
controller E1 0/15
framing NO-CRC4
clock source line
cem-group 0 timeslots 1-31
description TDM Shorthaul for CESoPSN PW
!
interface Loopback0
description Loopback for MPLS and PWE3
ip address 10.10.10.1 255.255.255.255
!
interface CEM0/15
description CESoPSN
no ip address
cem 0
xconnect 10.10.10.2 111 encapsulation mpls
!
!
interface Tunnel3
ip address 9.9.9.9 255.255.255.0
tunnel mode gre ip
mpls ip
tunnel source Vlan3
tunnel destination 3.3.3.3
!
ip route 10.10.10.2 255.255.255.255 9.9.9.1
!
mpls ldp router-id Loopback0 force
!
```

## ATM over MPLS AAL5 SDU Mode with GRE Backhaul

```

!
interface ATM0/0
no ip address
scrambling-payload
no atm ilmi-keepalive
pvc 0/10 12transport
encapsulation aal5
xconnect 10.10.10.1 300 encapsulation mpls
!
interface Tunnel3
ip address 9.9.9.9 255.255.255.0
tunnel mode gre ip
mpls ip
tunnel source Vlan3
tunnel destination 3.3.3.3
!
interface Loopback0
description Loopback for MPLS and PWE3
ip address 10.10.10.1 255.255.255.255
!
ip route 10.10.10.1 255.255.255.255 9.9.9.1
!
mpls ldp router-id Loopback0 force

```

## Routing Sample Configurations

The following section contains sample configurations for each routing protocol using BFD.

- [OSPF with BFD](#)
- [BGP with BFD](#)
- [IS-IS with BFD](#)

For more information about how to configure routing on the Cisco MWR 2941, see [Configuring Routing Protocols, page 4-59](#) and [Configuring BFD, page 4-59](#).

### OSPF with BFD

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BFD2941
!
boot-start-marker
boot-end-marker
!
card type t1 0 0
logging buffered 1000000
no logging console
!
no aaa new-model
ip source-route
!
!

```

```

ip cef
no ip domain lookup
ip host tftp 64.102.116.25
ptp mode ordinary
ptp priority1 128
ptp priority2 128
ptp domain 0
multilink bundle-name authenticated
!
archive
  log config
  hidekeys
!
controller T1 0/0
  mode atm
  clock source line
!
controller T1 0/1
  clock source line
  cem-group 0 timeslots 1-31
!
controller T1 0/2
  clock source internal
!
controller T1 0/3
  clock source internal
!
controller T1 0/4
  clock source internal
!
controller T1 0/5
  clock source internal
!
controller T1 0/6
  clock source internal
!
controller T1 0/7
  clock source internal
!
controller T1 0/8
  clock source internal
!
controller T1 0/9
  clock source internal
!
controller T1 0/10
  clock source internal
!
controller T1 0/11
  clock source internal
!
controller T1 0/12
  clock source internal
!
controller T1 0/13
  clock source internal
!
controller T1 0/14
  clock source internal
!
controller T1 0/15
  clock source internal
!
controller BITS

```



```
    applique E1
!
!
interface Loopback0
 ip address 88.88.88.150 255.255.255.255
!
interface GigabitEthernet0/0
 switchport trunk allowed vlan 1-9,11-4094
 switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
 switchport access vlan 10
!
interface GigabitEthernet0/3
!
interface GigabitEthernet0/4
!
interface GigabitEthernet0/5
!
interface ATM0/0
 no ip address
 scrambling-payload
 atm pvp 1 l2transport
  xconnect 10.10.10.2 10001 encapsulation mpls
 no atm ilmi-keepalive
 pvc 0/20 l2transport
  vc-hold-queue 80
  encapsulation aal0
  xconnect 10.10.10.2 10020 encapsulation mpls
!
 pvc 0/30 l2transport
  encapsulation aal5
  xconnect 10.10.10.2 10030 encapsulation mpls
!
 pvc 0/40
  vc-hold-queue 50
  encapsulation aal5snap
!
!
interface CEM0/1
 no ip address
 cem 0
  xconnect 10.10.10.2 222 encapsulation mpls
!
!
interface Vlan1
 no ip address
 shutdown
 no ptp enable
!
interface Vlan10
 ip address 192.168.52.88 255.255.255.0
 no ptp enable
!
interface Vlan100
 description Primary EVC
 ip address 172.22.41.2 255.255.255.0
 ip ospf cost 4
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 no ptp enable
 mpls ip
```

```
    bfd interval 50 min_rx 50 multiplier 3
    !
interface Vlan200
  description Secondary EVC
  ip address 172.22.42.2 255.255.255.0
  ip ospf cost 5
  ip ospf hello-interval 1
  ip ospf dead-interval 3
  no ptp enable
  mpls ip
  !
router ospf 100
  router-id 88.88.88.150
  log-adjacency-changes
  timers throttle spf 50 50 1000
  timers throttle lsa all 0 25 10000
  timers lsa arrival 0
  timers pacing flood 20
  timers pacing retransmission 30
  redistribute static subnets
  network 88.88.88.150 0.0.0.0 area 0
  network 172.22.41.0 0.0.0.255 area 0
  network 172.22.42.0 0.0.0.255 area 0
  bfd all-interfaces
  !
ip default-gateway 192.168.52.1
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.52.1
ip route 64.102.116.25 255.255.255.255 192.168.52.1
  !
  !
ip http server
no ip http secure-server
  !
control-plane
  !
line con 0
  exec-timeout 0 0
  no modem enable
line aux 0
line vty 0 4
  exec-timeout 0 0
  privilege level 15
  password xxxxx
  login
  !
exception data-corruption buffer truncate
network-clock-select hold-timeout infinite
network-clock-select mode nonrevert
network-clock-select 1 E1 0/0
end
```

## BGP with BFD

```
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname BFD2941  
!  
boot-start-marker  
boot-end-marker  
!  
card type t1 0 0  
logging buffered 1000000  
no logging console  
!  
no aaa new-model  
ip source-route  
!  
!  
ip cef  
no ip domain lookup  
ip host tftp 64.102.116.25  
ptp mode ordinary  
ptp priority1 128  
ptp priority2 128  
ptp domain 0  
multilink bundle-name authenticated  
!  
archive  
  log config  
  hidekeys  
!  
controller T1 0/0  
  mode atm  
  clock source line  
!  
controller T1 0/1  
  clock source line  
  cem-group 0 timeslots 1-31  
!  
controller T1 0/2  
  clock source internal  
!  
controller T1 0/3  
  clock source internal  
!  
controller T1 0/4  
  clock source internal  
!  
controller T1 0/5  
  clock source internal  
!  
controller T1 0/6  
  clock source internal  
!  
controller T1 0/7  
  clock source internal  
!  
controller T1 0/8  
  clock source internal  
!
```

```

controller T1 0/9
  clock source internal
!
controller T1 0/10
  clock source internal
!
controller T1 0/11
  clock source internal
!
controller T1 0/12
  clock source internal
!
controller T1 0/13
  clock source internal
!
controller T1 0/14
  clock source internal
!
controller T1 0/15
  clock source internal
!
controller BITS
  applique E1
!
interface Loopback0
  ip address 20.20.20.20 255.255.255.255
!
interface GigabitEthernet0/2
  switchport access vlan 10
  load-interval 30
  duplex full
  speed 100
!
interface GigabitEthernet0/3
  switchport access vlan 200
  load-interval 30
  duplex full
  speed 100
!
interface GigabitEthernet0/4
  switchport access vlan 4
  load-interval 30
  duplex full
  speed 100
!
interface GigabitEthernet0/5
  switchport access vlan 100
  load-interval 30
  duplex full
  speed 100
!
interface ATM0/0
  no ip address
  scrambling-payload
  atm bandwidth dynamic
  pvc 0/100 l2transport
!
!
interface ATM0/0.1 multipoint
  pvc 1/5 l2transport
  encapsulation aal0
  xconnect 10.10.10.10 10010 encapsulation mpls
!
pvc 1/6 l2transport

```

```
        encapsulation aal5
        xconnect 10.10.10.10 10020 encapsulation mpls
    !
    !
interface ATM0/0.2 multipoint
    xconnect 10.10.10.10 10030 encapsulation mpls
    pvc 2/5 l2transport
        encapsulation aal0
    !
    pvc 2/6 l2transport
        encapsulation aal0
    !
    !
interface ATM0/1
    no ip address
    scrambling-payload
    no atm ilmi-keepalive
    pvc 0/100 l2transport
    !
    !
interface Vlan4 (connected to 7600)
    ip address 11.1.1.2 255.255.255.0
    no ptp enable
    bfd interval 50 min_rx 50 multiplier 3
    !
interface Vlan10
    ip address 192.168.40.61 255.255.255.128
    no ptp enable
    mpls ip
    !
interface Vlan100
    ip address 12.1.1.2 255.255.255.0
    no ptp enable
    mpls bgp forwarding
    mpls ip
    bfd interval 50 min_rx 50 multiplier 3
    !
interface Vlan200
    ip address 12.1.2.2 255.255.255.0
    no ptp enable
    mpls bgp forwarding
    mpls ip
    bfd interval 50 min_rx 50 multiplier 3
    !
router bgp 200
    no synchronization
    bgp log-neighbor-changes
    network 11.1.1.0
    network 12.1.1.0
    network 12.1.2.0
    redistribute connected
    neighbor 11.1.1.1 remote-as 100
    neighbor 11.1.1.1 fall-over bfd
    neighbor 11.1.1.1 send-label
    neighbor 12.1.1.1 remote-as 300
    neighbor 12.1.1.1 fall-over bfd
    neighbor 12.1.1.1 send-label
    neighbor 12.1.2.1 remote-as 300
    neighbor 12.1.2.1 fall-over bfd
    neighbor 12.1.2.1 send-label
    no auto-summary
    !
connect atmcellsw ATM0/0 0/100 ATM0/1 0/100
    !
```

```
!  
mpls ldp router-id Loopback0 force  
!
```

## IS-IS with BFD

```
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname BFD2941  
!  
boot-start-marker  
boot-end-marker  
!  
card type t1 0 0  
logging buffered 1000000  
no logging console  
!  
no aaa new-model  
ip source-route  
!  
!  
ip cef  
no ip domain lookup  
ip host tftp 64.102.116.25  
ptp mode ordinary  
ptp priority1 128  
ptp priority2 128  
ptp domain 0  
multilink bundle-name authenticated  
!  
archive  
  log config  
  hidekeys  
!  
controller T1 0/0  
  mode atm  
  clock source line  
!  
controller T1 0/1  
  clock source line  
  cem-group 0 timeslots 1-31  
!  
controller T1 0/2  
  clock source internal  
!  
controller T1 0/3  
  clock source internal  
!  
controller T1 0/4  
  clock source internal  
!  
controller T1 0/5  
  clock source internal  
!  
controller T1 0/6  
  clock source internal  
!
```

```
controller T1 0/7
  clock source internal
!
controller T1 0/8
  clock source internal
!
controller T1 0/9
  clock source internal
!
controller T1 0/10
  clock source internal
!
controller T1 0/11
  clock source internal
!
controller T1 0/12
  clock source internal
!
controller T1 0/13
  clock source internal
!
controller T1 0/14
  clock source internal
!
controller T1 0/15
  clock source internal
!
controller BITS
  applique E1
!
interface Loopback0
  ip address 20.20.20.20 255.255.255.255
!
interface GigabitEthernet0/2
  switchport access vlan 10
  load-interval 30
  duplex full
  speed 100
!
interface GigabitEthernet0/3
  switchport access vlan 200
  load-interval 30
  duplex full
  speed 100
!
interface GigabitEthernet0/4
  switchport access vlan 4
  load-interval 30
  duplex full
  speed 100
!
interface GigabitEthernet0/5
  switchport access vlan 100
  load-interval 30
  duplex full
  speed 100
!
interface ATM0/0
  no ip address
  scrambling-payload
  atm bandwidth dynamic
pvc 0/100 12transport
!
!
```

```

interface ATM0/0.1 multipoint
  pvc 1/5 l2transport
    encapsulation aal0
    xconnect 10.10.10.10 10010 encapsulation mpls
  !
  pvc 1/6 l2transport
    encapsulation aal5
    xconnect 10.10.10.10 10020 encapsulation mpls
  !
  !
interface ATM0/0.2 multipoint
  xconnect 10.10.10.10 10030 encapsulation mpls
  pvc 2/5 l2transport
    encapsulation aal0
  !
  pvc 2/6 l2transport
    encapsulation aal0
  !
  !
interface ATM0/1
  no ip address
  scrambling-payload
  no atm ilmi-keepalive
  pvc 0/100 l2transport
  !
  !
interface Vlan4
  ip address 11.1.1.2 255.255.255.0
  ip router isis test_ip_isis
  no ptp enable
  isis bfd
  !
interface Vlan10
  ip address 192.168.40.61 255.255.255.128
  no ptp enable
  mpls ip
  !
interface Vlan100
  ip address 12.1.1.2 255.255.255.0
  ip router isis test_ip_isis
  no ptp enable
  mpls ip
  bfd interval 50 min_rx 50 multiplier 3
  isis bfd
  !
interface Vlan200
  ip address 12.1.2.2 255.255.255.0
  ip router isis test_ip_isis
  no ptp enable
  mpls ip
  bfd interval 50 min_rx 50 multiplier 3
  isis bfd
  !
router isis test_ip_isis
  net 47.0004.004d.0055.0000.0c00.0002.00
  net 47.0004.004d.0056.0000.0c00.0002.00
  is-type level-2-only
  redistribute connected
  bfd all-interfaces
  !

```



## Multicast Sample Configurations

The following sample configurations show how to configure multicast on the Cisco MWR 2941.

**Note**

These sections provide partial configurations in order to demonstrate a specific feature.

- [Sparse Mode with a Static Rendezvous Point](#)
- [Source-Specific Multicast](#)

### Sparse Mode with a Static Rendezvous Point

```
!  
ip multicast-routing  
!  
interface VLAN2  
  description Ethernet Backhaul  
  ip pim sparse-mode  
  ip pim query-interval 2  
  ip pim version 2  
!  
interface VLAN3  
  description Ethernet Shorthaul  
  ip pim sparse-mode  
  ip pim version 2  
  ip igmp query-max-response-time 5  
  ip igmp query-interval 7  
!  
ip pim register-source Loopback0  
ip pim rp-address 1.1.1.1 2 override  
!  
access-list 2 permit 239.193.0.0 0.0.255.255  
access-list 2 permit 239.194.0.0 0.0.255.255  
!
```

### Source-Specific Multicast

```
!  
ip multicast-routing  
!  
interface VLAN2  
  description Ethernet Backhaul  
  ip pim sparse-mode  
  ip pim query-interval 2  
  ip pim version 2  
!  
interface VLAN3  
  description Ethernet Shorthaul  
  ip pim sparse-mode  
  ip pim version 2  
  ip pim bsr-border  
  ip igmp static-group 239.193.0.3 source 10.234.0.125  
  ip igmp static-group 239.193.0.3 source 10.234.45.133  
  ip igmp static-group 239.193.0.3 source 10.234.45.137  
  ip igmp static-group 239.193.0.3 source 10.234.45.141  
  ip igmp static-group 239.193.0.3 source 10.234.45.129  
  ip igmp static-group 239.193.0.12 source 10.234.0.125
```

```
ip igmp static-group 239.193.0.12 source 10.234.45.133
ip igmp static-group 239.193.0.12 source 10.234.45.137
ip igmp static-group 239.193.0.12 source 10.234.45.141
ip igmp static-group 239.193.0.12 source 10.234.45.129
ip igmp query-max-response-time 5
ip igmp query-interval 7
!
ip access-list standard SSM
 permit 239.193.0.0 0.0.255.255
 permit 239.194.0.0 0.0.255.255
!
ip pim register-source Loopback0
ip pim ssm range SSM
!
```

For more information about how to configure multicast, see [Configuring IP Multicast, page 4-64](#).

## PTP Sample Configurations

The following sections show a sample configurations for PTP. For more information about how to configure PTP, see [Configuring Clocking and Timing, page 4-39](#).

- [PTP Slave Mode with Redundancy](#)
- [PTP Redundancy](#)
- [PTP Hybrid Mode](#)
- [PTP Hot Standby Master Clock](#)
- [PTP Input Timing](#)
- [PTP Output Timing](#)

### PTP Slave Mode with Redundancy

The following configuration implements PTP slave mode and PTP redundancy.

```
!
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname MWR_2
!
boot-start-marker
boot system flash mwr2941-ipran-mz.ricwest-ntp
boot-end-marker
!
card type e1 0 0
enable secret 5 mysecret
!
no aaa new-model
ip source-route
!
!
ip cef
no ip domain lookup
ip multicast-routing
ptp mode ordinary
ptp priority1 128
ptp priority2 128
```

```
ptp domain 0
multilink bundle-name authenticated
!
mpls label protocol ldp
!
!
ipran-mib snmp-access outOfBand
archive
  log config
  hidekeys
!
!
controller E1 0/0
  clock source internal
  cem-group 0 unframed
  description TDM Shorthaul for SAToP PW
!
controller E1 0/1
  framing NO-CRC4
  clock source internal
  cem-group 0 timeslots 1-31
  description TDM Shorthaul for CESoPSN PW
!
controller E1 0/2
  clock source internal
!
controller E1 0/3
  clock source internal
!
controller E1 0/4
  clock source line
!
controller E1 0/5
  clock source line
!
controller E1 0/6
  clock source line
!
controller E1 0/7
  clock source line
!
controller E1 0/8
  clock source internal
  ima-group 0 scrambling-payload
  description ATM Shorthaul for ATMOMPLS PW
!
controller E1 0/9
  clock source internal
  ima-group 0 scrambling-payload
  description ATM Shorthaul for ATMOMPLS PW
!
controller E1 0/10
  clock source internal
  ima-group 0 scrambling-payload
  description ATM Shorthaul for ATMOMPLS PW
!
controller E1 0/11
  clock source internal
!
controller E1 0/12
  clock source internal
!
controller E1 0/13
  clock source internal
```

```
!  
controller E1 0/14  
    clock source internal  
!  
controller E1 0/15  
    clock source internal  
!  
controller BITS  
    applique E1  
!  
!  
pseudowire-class My_MPLS  
    encapsulation mpls  
    sequencing both  
!  
!  
interface Loopback0  
    ip address 10.1.1.22 255.255.255.255  
!  
interface GigabitEthernet0/0  
    switchport access vlan 11  
!  
interface GigabitEthernet0/1  
    switchport access vlan 12  
!  
interface GigabitEthernet0/2  
    switchport access vlan 30  
!  
interface GigabitEthernet0/3  
    shutdown  
!  
interface GigabitEthernet0/4  
    switchport mode trunk  
    shutdown  
!  
interface GigabitEthernet0/5  
    switchport access vlan 5  
    duplex full  
    speed 1000  
!  
interface CEM0/0  
    description SAToP PW  
    no ip address  
    cem 0  
    xconnect 10.10.10.36 5200 encapsulation mpls  
!  
!  
interface CEM0/1  
    description CESoPSN PW  
    no ip address  
    cem 0  
    xconnect 10.10.10.36 5201 encapsulation mpls  
!  
!  
interface ATM0/IMA0  
    description ATMoMPLS N:1 VCC Mode (where N=1)  
    no ip address  
    ima group-id 0  
    atm bandwidth dynamic  
    no atm ilmi-keepalive  
    pvc 1/32 l2transport  
    encapsulation aal5  
    xconnect 10.10.10.36 5232 encapsulation mpls  
!
```

```
pvc 1/36 l2transport
 encapsulation aal0
 xconnect 10.10.10.36 5236 encapsulation mpls ignore-vpi-vci
 !
pvc 1/37 l2transport
 encapsulation aal0
 xconnect 10.10.10.36 5237 encapsulation mpls ignore-vpi-vci
 !
pvc 1/38 l2transport
 encapsulation aal0
 xconnect 10.10.10.36 5238 encapsulation mpls ignore-vpi-vci
 !
pvc 1/39 l2transport
 encapsulation aal0
 xconnect 10.10.10.36 5239 encapsulation mpls ignore-vpi-vci
 !
!
interface Vlan1
 no ip address
 shutdown
 no ptp enable
 !
interface Vlan3
 description 7600/2941 MPLS Backhaul VLAN
 ip address 192.22.2.2 255.255.255.0
 ip pim sparse-mode
 ptp sync interval -6
 ptp delay-req interval -4
 ptp slave multicast
 ptp enable
 mpls ip
 !
interface Vlan5
 ip address 192.18.75.38 255.255.255.0
 no ptp enable
 !
interface Vlan11
 description Link to 7600-PE1
 ip address 10.100.11.2 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
 no ptp enable
 mpls ip
 !
interface Vlan12
 description Link to 7600-PE2
 ip address 10.100.12.2 255.255.255.252
 ip pim sparse-mode
 ip igmp join-group 224.0.1.129 source 10.100.2.2
 ip igmp join-group 224.0.1.129 source 10.100.3.2
 ip ospf 1 area 0
 no ptp enable
 mpls ip
 !
interface Vlan30
 description Link to PTP client
 ip address 10.100.30.1 255.255.255.0
 ip pim sparse-mode
 no ptp enable
 !
router ospf 1
 router-id 10.1.1.22
 log-adjacency-changes
 redistribute connected subnets
```

```
network 10.1.1.22 0.0.0.0 area 0
network 10.1.11.0 0.0.0.3 area 0
network 10.1.12.0 0.0.0.3 area 0
network 10.100.30.0 0.0.0.255 area 0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 172.18.75.1
ip route 10.1.1.201 255.255.255.255 10.100.11.1
ip route 10.1.1.202 255.255.255.255 10.100.12.1
!
!
ip http server
ip pim rp-address 10.2.1.1 5 override
!
access-list 5 permit 224.0.1.129
snmp-server community public RO 1
snmp-server ifindex persist
snmp-server trap link ietf
no snmp-server sparse-tables
snmp-server queue-limit notification-host 100
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps cpu threshold
snmp-server enable traps syslog
snmp-server enable traps ipran
snmp-server host 10.10.10.10 version 2c V2C
!
!
!
mpls ldp router-id Loopback0 force
!
control-plane
!
!
!
!
!
!
line con 0
  logging synchronous
  no modem enable
line aux 0
line vty 0 4
  password mypassword
  login
!
exception data-corruption buffer truncate
ntp clock-period 17180198
ntp peer 10.81.254.131
network-clock-select hold-timeout 600
network-clock-select mode nonrevert
network-clock-select 1 PACKET-TIMING
end
```

## PTP Redundancy

The following configurations use PTP with PTP redundancy.

**Note**

This section provides partial configurations intended to demonstrate a specific feature.

**MWR\_A**

```
!  
interface Loopback0  
ip address 6.6.6.3 255.255.255.255  
end  
!  
interface GigabitEthernet0/0  
switchport access vlan 10  
!  
interface GigabitEthernet0/1  
switchport access vlan 5  
!  
interface Vlan5  
ip address 5.5.5.2 255.255.255.0  
ip router isis  
ip pim sparse-mode  
no ptp enable  
!  
interface Vlan10  
ip address 10.10.10.2 255.255.255.0  
ip router isis  
ip pim sparse-mode  
no ptp enable  
!  
router isis  
net 49.0001.1720.1600.3003.00  
passive-interface Loopback0  
!  
ip pim rp-address 6.6.6.1 override  
!
```

**MWR\_B**

```
!  
interface Loopback0  
ip address 6.6.6.2 255.255.255.255  
ip pim sparse-mode  
end  
!  
interface GigabitEthernet0/0  
switchport access vlan 10  
!  
interface GigabitEthernet0/4  
switchport access vlan 4  
load-interval 30  
!  
!  
interface Vlan4  
ip address 7.7.7.2 255.255.255.0  
ip router isis  
ip pim sparse-mode  
no ptp enable  
!  
!
```

```
interface Vlan10
ip address 10.10.10.1 255.255.255.0
ip router isis
ip pim sparse-mode
no ptp enable
!
router isis
net 49.0001.1720.1600.9009.00
passive-interface Loopback0
!
ip pim rp-address 6.6.6.1 override
```

## PTP Hybrid Mode

The following section shows a sample PTP configuration that uses hybrid mode. For more information about how to configure PTP hybrid mode, see [Configuring PTP Clocking, page 4-39](#).

**Note**

---

This section provides a partial configuration intended to demonstrate a specific feature.

---

```
ptp mode ordinary
ptp priority1 128
ptp priority2 128
ptp domain 1

interface Vlan1
ip address 192.168.1.2 255.255.255.0
ptp announce interval 3
ptp announce timeout 2
ptp sync interval -4
ptp delay-req interval -4
ptp slave multicast hybrid
ptp enable

network-clock-select 1 SYNCE 0/1
```

## PTP Hot Standby Master Clock

The following section shows a sample PTP configuration that uses a hot standby master clock. For more information about how to configure a PTP hot standby master clock, see [Configuring PTP Clocking, page 4-39](#).

**Note**

---

This section provides a partial configuration intended to demonstrate a specific feature.

---

```
ptp mode ordinary
ptp priority1 128
ptp priority2 128
ptp domain 1
ptp best-recovered-quality 2 30

interface Vlan1
ip address 192.168.1.2 255.255.255.0
ptp announce interval 3
ptp announce timeout 2
```



```
ptp sync interval -4
ptp delay-req interval -4
ptp slave unicast negotiation
ptp clock-source 10.0.1.2
ptp clock-source 10.0.1.3
ptp enable

network-clock-select 1 PACKET_TIMING
```

## PTP Input Timing

The following sample configuration sets the router as a PTP master clock with input timing enabled using the 10Mhz timing port.

**Note**

This section only applies to the Cisco MWR 2941-DC-A router; the Cisco MWR-DC router does not have the timing ports used in this example.

**Note**

This section provides a partial configuration intended to demonstrate a specific feature.

```
ptp mode ordinary
ptp priority1 128
ptp priority2 128
ptp domain 0
ptp input 10M 1pps
ptp tod iso
ptp update-calendar

interface GigabitEthernet 0/0
    switchport access vlan 1588

interface vlan 1588
    ip address 192.168.15.89 255.255.255.0
    ip igmp join-group 224.0.1.129
    ptp sync interval -6
    ptp delay-req interval -4
    ptp master multicast
    ptp enable

network-clock-select hold-timeout 3600
network-clock-select 1 10M
```

## PTP Output Timing

The following sample configuration sets the router as a PTP slave clock with output timing enabled on the 10M timing port.

**Note**

This section only applies to the Cisco MWR 2941-DC-A router.; the Cisco MWR-DC router does not have the timing ports used in this example.

**Note**

This section provides a partial configuration intended to demonstrate a specific feature.

```
ptp mode ordinary
ptp priority1 128
ptp priority2 128
ptp domain 0
ptp output 10M 1pps
ptp tod ubx delay 1
ptp update-calendar

interface GigabitEthernet 0/0
    switchport access vlan 1588

interface vlan 1588
    ip address 192.168.15.88 255.255.255.0
    ip igmp join-group 224.0.1.129
    ptp sync interval -6
    ptp delay-req interval -4
    ptp slave multicast
    ptp enable

network-clock-select hold-timeout 1000
network-clock-select 1 PACKET-TIMING
enable 10M
```

## Layer 3 VPN Sample Configuration

The following section shows a sample configuration for Layer 3 Virtual Private Network (VPN). For more information about how to configure Layer 3 VPNs, see [Configuring Layer 3 Virtual Private Networks \(VPNs\)](#), page 4-88.

**Note**

This section provides a partial configuration intended to demonstrate a specific feature.

```
!
-----Customer definitions for 2 customers-----
vrf definition customer_a
rd 192.168.1.1:100
route-target export 192.168.1.1:100
route-target import 192.168.1.1:100
!
address-family ipv4
exit-address-family
!
vrf definition customer_b
rd 192.168.2.1:200
route-target export 192.168.2.1:200
```

```

route-target import 192.168.2.1:200
!
address-family ipv4
exit-address-family
!
-----Loopback addresses for 2 customers-----
interface Loopback100
vrf forwarding customer_a
ip address 192.169.1.3 255.255.255.255
!
interface Loopback101
vrf forwarding customer_b
ip address 192.168.100.1 255.255.255.255
!
-----Core-facing OSPF instance-----
router ospf 1
log-adjacency-changes
network 100.0.0.0 0.255.255.255 area 0
network 192.168.0.0 0.0.255.255 area 0
network 192.169.0.0 0.0.255.255 area 0
!
-----VRF OSPF instances for 2 customers -----
router ospf 100 vrf customer_a
router-id 192.168.1.3
log-adjacency-changes
redistribute bgp 101 metric-type 1 subnets
network 192.168.0.0 0.0.255.255 area 0
network 192.169.0.0 0.0.255.255 area 0
!
router ospf 100 vrf customer_b
router-id 192.168.100.1
log-adjacency-changes
redistribute bgp 101 metric-type 1 subnets
network 192.168.0.0 0.0.255.255 area 0
network 192.169.0.0 0.0.255.255 area 0
!
-----MP-BGP with 2 VRF customers -----
router bgp 101
bgp router-id 100.1.1.1
bgp log-neighbor-changes
neighbor 100.1.1.2 remote-as 101
neighbor 100.1.1.2 update-source Loopback1
!
address-family ipv4
redistribute connected
neighbor 100.1.1.2 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 100.1.1.2 activate
neighbor 100.1.1.2 send-community extended
bgp scan-time import 5
exit-address-family
!
address-family ipv4 vrf customer_b
redistribute connected
neighbor 100.1.1.2 remote-as 101
neighbor 100.1.1.2 update-source Loopback1
neighbor 100.1.1.2 activate
no synchronization
exit-address-family
!

```

```

address-family ipv4 vrf customer_a
redistribute connected
neighbor 100.1.1.2 remote-as 101
neighbor 100.1.1.2 update-source Loopback1
neighbor 100.1.1.2 activate
no synchronization
exit-address-family
!
-----MP-BGP loopback interface -----
interface Loopback1
ip address 100.1.1.1 255.255.255.255
!
-----Core-facing Vlan interface -----
interface GigabitEthernet0/1
switchport access vlan 20
switchport trunk allowed vlan 1,2,20-23,1002-1005
switchport mode trunk
load-interval 30
!
interface Vlan20
ip address 192.169.10.1 255.255.255.0
load-interval 30
no ptp enable
mpls ip
!
-----CE-facing Vlan interfaces for 2 customers-----
interface GigabitEthernet0/4
switchport access vlan 100
load-interval 30
duplex full
!
interface Vlan100
vrf forwarding customer_a
ip address 192.169.3.2 255.255.255.0
!
interface GigabitEthernet0/5
switchport access vlan 99
load-interval 30
duplex full
!
interface Vlan99
vrf forwarding customer_b
ip address 192.169.3.2 255.255.255.0
!

```

## QoS Sample Configurations

The following sample configurations demonstrate how you can apply QoS configurations on the Cisco MWR 2941.



### Note

This section provides partial configurations intended to demonstrate a specific feature.

The following sections provide sample configurations for QoS on the Cisco MWR 2941.

- [Switchport Priority](#)
- [Classification and Marking](#)
- [Priority Queuing](#)

For more information about configuring QoS, see [Configuring Quality of Service \(QoS\)](#), page 4-88.

## Switchport Priority

The following sample configuration demonstrates how to mark P-bit values on incoming traffic on the 9ESW HWIC interface.

```
.....
interface GigabitEthernet0/2
no ip address
  switchport stacking-partner interface FastEthernet1/8
.....
interface FastEthernet1/7
switchport mode trunk
switchport priority override 7    ! set all ingress traffic to priority 7
                                   ! regardless of current priority values.

interface FastEthernet1/7
switchport mode access
switchport access vlan 100
switchport priority default 5    ! set all ingress traffic to priority 5

interface FastEthernet1/8
no IP address
switchport stacking-partner interface GigabitEthernet0/2
```

## Classification and Marking

The following configuration example marks the DSCP value of ingress Ethernet traffic and assigns it to a QoS group, and marks P-bits. Egress traffic is queued using WRR with bandwidth percentages allocated to each group.

```
! Note 1: these class-maps are applied on ingress
class-map match-any common-channels
  match dscp af31 af32 af33
class-map match-any HSDPA
  match dscp default
class-map match-any R99
  match dscp af21 af22 af23
class-map match-any synchronization
  match dscp ef cs6
class-map match-any signaling
  match dscp af41 af42 af43
!
! Note 2: these class-maps are applied on egress
class-map match-any group1
  match qos-group 1
class-map match-any group2
  match qos-group 2
class-map match-any group3
  match qos-group 3
class-map match-any group4
  match qos-group 4
class-map match-any group5
  match qos-group 5
class-map match-any group6
  match qos-group 6

! Note 3: The input policy performs the DSCP match and all marking
policy-map input-policy
  class synchronization
```

```

    set qos-group 6
    set cos 6
class signaling
    set qos-group 5
    set cos 5
class common-channels
    set qos-group 4
    set cos 4
class R99
    set qos-group 3
    set cos 3
class HSDPA
    set qos-group 1
class default
    set qos-group 1
!
! Note 4: the hierarchical output policy handles WRR and shaping
policy-map QOS-child
class group6
    priority percent 5
class group5
    bandwidth percent 20
class group4
    bandwidth percent 20
class group3
    bandwidth percent 20
class group1
    bandwidth percent 20
policy-map output-policy
class class-default
    shape average 38000000
    service-policy QOS-child
!
Interface GigabitEthernet 0/0
    service-policy input input-policy
Interface GigabitEthernet 0/1
    service-policy output output-policy

```

## MPLS Bit Marking

The following configuration example marks MPLS Exp bits on traffic passing through pseudowire class UMTS\_3. You can map the Exp bit value to a QoS group on an MLPPP egress interface or an MLPPP or layer 2 Ethernet queue.

```

!
pseudowire-class UMTS_3
encapsulation mpls
mpls experimental 3
!
interface ATM0/IMA0
pvc 2/1 l2transport
encapsulation aal0
xconnect 10.10.10.1 121 pw-class UMTS_3
!
!

```

## Priority Queuing

The following sample configuration places any traffic with a DSCP value of **ef** into the priority queue of the MLPPP multilink interface.

```
class-map match-any gsm-abis
  match dscp ef
!
!
policy-map gsm-abis ? note that without multiclass up to 4 queues supported
  class gsm-abis
    priority percent 99
  class class-default
    bandwidth remaining percent 1
!

interface Multilink1
ip address 50.50.50.49 255.255.255.0
load-interval 30
keepalive 1
ppp pfc local request
ppp pfc remote apply
ppp acfc local request
ppp acfc remote apply
ppp multilink
ppp multilink interleave
ppp multilink group 1
ppp multilink fragment delay 0 1
ppp multilink multiclass
ppp timeout multilink lost-fragment 1
max-reserved-bandwidth 100
service-policy output gsm-abis
hold-queue 50 out
```

## Resilient Ethernet Protocol (REP) Sample Configuration

The following configuration example shows two Cisco MWR 2941 routers and two Cisco 7600 series routers using a REP ring.



### Note

This section provides partial configurations intended to demonstrate a specific feature.

### 2941\_1

```
interface GigabitEthernet0/0
  switchport trunk allowed vlan 1,2
  switchport mode trunk
  rep segment 1
!
interface GigabitEthernet0/1
  switchport trunk allowed vlan 1,2
  switchport mode trunk
  rep segment 1
!
interface GigabitEthernet0/3
  switchport access vlan 3
!
```

```
interface GigabitEthernet0/4
  switchport access vlan 4
!
interface Vlan1
  ip address 172.18.40.70 255.255.255.128
  no ptp enable
!
interface Vlan2
  ip address 1.1.1.1 255.255.255.0
  no ptp enable
!
interface Vlan3
  ip address 2.2.2.2 255.255.255.0
  no ptp enable
!
interface Vlan3
  ip address 4.4.4.2 255.255.255.0
  no ptp enable
!
ip route 3.3.3.0 255.255.255.0 1.1.1.4
ip route 5.5.5.0 255.255.255.0 1.1.1.4
```

## 2941\_2

```
interface GigabitEthernet0/0
  switchport trunk allowed vlan 1,2
  switchport mode trunk
  rep segment 1
!
interface GigabitEthernet0/1
  switchport trunk allowed vlan 1,2
  switchport mode trunk
  rep segment 1
!
interface Vlan1
  ip address 172.18.44.239 255.255.255.0
  no ptp enable
!
interface Vlan2
  ip address 1.1.1.2 255.255.255.0
  no ptp enable
```

## 7600\_1

```
interface Port-channel69
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,2
  switchport mode trunk
!
interface GigabitEthernet3/25
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,2
  switchport mode trunk
  channel-group 69 mode on
!
interface GigabitEthernet3/26
```



```
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
channel-group 69 mode on
!
interface GigabitEthernet3/35
ip address 3.3.3.2 255.255.255.0
!
interface GigabitEthernet3/36
ip address 5.5.5.2 255.255.255.0
!
interface GigabitEthernet5/2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
rep segment 1 edge
!
interface Vlan1
no ip address
!
interface Vlan2
ip address 1.1.1.4 255.255.255.0
!
ip route 2.2.2.0 255.255.255.0 1.1.1.1
ip route 4.4.4.0 255.255.255.0 1.1.1.1
```

## 7600\_2

```
interface Port-channel69
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
!
interface GigabitEthernet5/2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
rep segment 1 edge
!
interface GigabitEthernet7/25
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
channel-group 69 mode on
!
interface GigabitEthernet7/26
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
channel-group 69 mode on
!
interface Vlan1
no ip address
!
interface Vlan2
```

```
ip address 1.1.1.3 255.255.255.0
!
```

## Cisco Networking Services (CNS) Zero Touch Deployment Configuration

The following configuration example sets the Cisco MWR 2941 to boot using configurations stored on a CNS-CE server with the IP address 30.30.1.20. For more information about configuring CNS, see [Configuring Cisco Networking Services \(CNS\), page 4-115](#).

**Note**

---

This section provides partial configurations intended to demonstrate a specific feature.

---

```
hostname 2941
!
cns trusted-server all-agents 30.30.1.20
cns event 30.30.1.20 11011 keepalive 60 3
cns config initial 30.30.1.20 80
cns config partial 30.30.1.20 80
cns id hostname
cns id hostname event
cns id hostname image
cns exec 80
logging buffered 20000
!
end
```

## CFM and ELMI Sample Configuration

The following sample configuration uses CFM and ELMI with three inward facing MEPs, two MIPs, and three maintenance domains.

**Note**

---

This section provides partial configurations intended to demonstrate a specific feature.

---

```
!
ethernet cfm ieee
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 112
ethernet cfm domain CISCO_7 level 7
  service L7 vlan 700
  continuity-check
!
ethernet cfm domain CISCO_ENG level 6
  service ce28 vlan 600
  continuity-check
!
ethernet cfm domain CISCO_5 level 5
  service L5 vlan 1
  continuity-check
!
ethernet lmi global
```

```
!  
interface GigabitEthernet0/2  
  switchport access vlan 600  
  shutdown  
  ethernet cfm mip level 7 vlan 600  
  ethernet cfm mep domain CISCO_ENG mpid 629 vlan 600  
!  
interface GigabitEthernet0/3  
  switchport mode trunk  
  shutdown  
  ethernet cfm mep domain CISCO_5 mpid 529 vlan 1  
!  
interface GigabitEthernet0/4  
  switchport access vlan 700  
  shutdown  
  ethernet cfm mep domain CISCO_7 mpid 729 vlan 700  
!  
interface GigabitEthernet0/5  
  switchport mode trunk  
  ethernet cfm mip level 5 vlan 1-2,100,600,700  
!
```





## APPENDIX **B**

# Cisco MWR 2941 Router Command Reference

---

This appendix contains an alphabetical listing of new and revised commands specific to the Cisco MWR 2941 router.



### Note

For a general reference for Cisco IOS, see the documentation for [Cisco IOS Software Releases 12.2 SR](#). The Cisco MWR 2941 does not necessarily support all of the commands listed in the 12.2SR documentation.

---

- [address-family ipv4 \(BGP\)](#)
- [alarm \(config-if-ecfm-mep mode\)](#)
- [atm ilmi-keepalive](#)
- [atm vc-per-vp](#)
- [backup delay](#)
- [backup peer](#)
- [bandwidth \(policy-map class\)](#)
- [bfd all-interfaces](#)
- [bfd interval](#)
- [cbr](#)
- [cdp enable](#)
- [cem-group](#)
- [class \(policy-map\)](#)
- [class cem](#)
- [class-map](#)
- [class-map type control](#)
- [class-map type traffic](#)
- [clear ethernet cfm errors](#)
- [clear ethernet cfm maintenance-points remote](#)
- [clear ethernet cfm statistics](#)
- [clear ethernet cfm traceroute-cache](#)
- [clock update-calendar](#)

- clock update-calendar
- controller
- cns config initial
- cns config partial
- cns config retrieve
- cns event
- cns exec
- cns id
- cns image password
- cns image retrieve
- cns inventory
- cns password
- cns template connect
- cns trusted-server
- dejitter-buffer
- dscp
- encapsulation (ATM)
- encapsulation (ATM)
- ethernet cfm cc
- ethernet cfm cc enable level vlan
- ethernet cfm domain level
- ethernet cfm enable
- ethernet cfm enable (interface)
- ethernet cfm logging
- ethernet cfm mep crosscheck
- ethernet cfm mep crosscheck start-delay
- ethernet cfm mep domain mpid
- ethernet cfm mep level mpid vlan
- ethernet cfm mip level
- ethernet cfm traceroute cache
- ethernet cfm traceroute cache hold-time
- ethernet cfm traceroute cache size
- ethernet lmi
- ethernet lmi global
- ethernet lmi interface
- ethernet oam
- ethernet oam link-monitor frame
- ethernet oam link-monitor frame-period

- [ethernet oam link-monitor frame-seconds](#)
- [ethernet oam link-monitor high-threshold action](#)
- [ethernet oam link-monitor on](#)
- [ethernet oam link-monitor receive-crc](#)
- [ethernet oam link-monitor supported](#)
- [ethernet oam link-monitor transmit-crc](#)
- [ethernet oam mib log size](#)
- [ethernet oam remote-failure action](#)
- [ethernet oam remote-loopback](#)
- [ethernet oam remote-loopback \(interface\)](#)
- [fair-queue \(class-default\)](#)
- [fair-queue \(policy-map class\)](#)
- [idle-pattern](#)
- [ima-group](#)
- [interface atm ima](#)
- [ip igmp join-group](#)
- [ip igmp query-interval](#)
- [ip igmp query-max-response-time](#)
- [ip igmp static-group](#)
- [ip igmp version](#)
- [ip local interface](#)
- [ip multicast-routing](#)
- [ip ospf bfd](#)
- [ip pim](#)
- [ip pim bsr-border](#)
- [ip pim bsr-candidate](#)
- [ip pim query-interval](#)
- [ip pim register-source](#)
- [ip pim rp-address](#)
- [ip pim rp-candidate](#)
- [ip pim send-rp-announce](#)
- [ip pim send-rp-discovery](#)
- [ip pim ssm](#)
- [ip pim version](#)
- [keepalive](#)
- [load-interval](#)
- [match any](#)
- [match atm clp](#)

- [match cos](#)
- [match dscp](#)
- [match ip dscp](#)
- [match mpls experimental](#)
- [match precedence](#)
- [match qos-group](#)
- [match vlan \(QoS\)](#)
- [maximum meps](#)
- [mdt data](#)
- [mdt default](#)
- [mep archive-hold-time](#)
- [mep crosscheck mpid vlan](#)
- [mode \(ATM/T1/E1 controller\)](#)
- [mpls ip \(global configuration\)](#)
- [mpls ip \(interface configuration\)](#)
- [mpls label](#)
- [mpls label range](#)
- [mpls ldp router-id](#)
- [neighbor \(OSPF\)](#)
- [neighbor remote-as \(BGP\)](#)
- [network-clock-select](#)
- [network-clock-select hold-timeout](#)
- [network-clock-select hold-off-timeout](#)
- [network-clock-select input-stratum4](#)
- [network-clock-select mode](#)
- [network-clock-select wait-to-restore-timeout](#)
- [payload-size](#)
- [ping ethernet](#)
- [ping ethernet vlan](#)
- [police \(percent\)](#)
- [police \(policy map\)](#)
- [police \(two rates\)](#)
- [police rate \(control-plane\)](#)
- [policy-map](#)
- [preferred-path](#)
- [priority](#)
- [protocol \(ATM\)](#)
- [pseudowire-class](#)



- `ptp announce`
- `ptp clock-destination`
- `ptp clock-source`
- `ptp delay-req interval`
- `ptp delay-req unicast`
- `ptp domain`
- `ptp enable`
- `ptp input`
- `ptp master`
- `ptp min-timing-pkt-size`
- `ptp mode`
- `ptp output`
- `ptp priority1`
- `ptp priority2`
- `ptp slave`
- `ptp sync interval`
- `ptp tod`
- `ptp two-steps`
- `ptp update-calendar`
- `pw-pvc`
- `ql-enabled rep segment`
- `queue-limit`
- `random-detect`
- `random-detect atm-clp-based`
- `random-detect cos-based`
- `random-detect discard-class`
- `random-detect discard-class-based`
- `random-detect dscp`
- `random-detect dscp (aggregate)`
- `random-detect ecn`
- `random-detect exponential-weighting-constant`
- `random-detect precedence-based`
- `recovered-clock slave`
- `rep admin vlan`
- `rep admin vlan`
- `rep block port`
- `rep preempt delay`
- `rep preempt segment`

- rep segment
- rep stcn
- router bgp
- router isis
- router ospf
- service (cfm-srv)
- service-policy
- service-policy (class-map)
- service-policy (policy-map class)
- set atm-clp
- set cos
- set cos-inner
- set cos-inner cos
- set discard-class
- set dscp
- set fr-de
- set ip dscp
- set ip dscp (policy-map configuration)
- set ip dscp tunnel
- set ip precedence (policy-map configuration)
- set ip precedence (policy-map)
- set ip precedence (route-map)
- set ip precedence tunnel
- set ip tos (route-map)
- set network-clocks
- set precedence
- set qos-group
- shape
- shape (percent)
- shape (policy-map class)
- shape max-buffers
- show adjacency
- show atm cell-packing
- show cem circuit
- show cem platform
- show connection
- show controller
- show cns config connections

- `show cns config outstanding`
- `show cns config stats`
- `show cns event connections`
- `show cns event stats`
- `show cns event subject`
- `show cns image connections`
- `show cns image inventory`
- `show cns image status`
- `show ethernet cfm domain`
- `show ethernet cfm domain`
- `show ethernet cfm errors`
- `show ethernet cfm maintenance-points local`
- `show ethernet cfm maintenance-points remote`
- `show ethernet cfm maintenance-points remote crosscheck`
- `show ethernet cfm maintenance-points remote detail`
- `show ethernet cfm statistics`
- `show ethernet cfm traceroute-cache`
- `show ethernet lmi`
- `show ethernet oam discovery`
- `show ethernet oam statistics`
- `show ethernet oam status`
- `show ethernet oam summary`
- `show interfaces rep`
- `show interface switchport backup`
- `show ip mroute`
- `show mpls l2transport vc`
- `show mpls l2transport vc`
- `show network-clocks`
- `show platform hardware`
- `show policy-map`
- `show policy-map interface`
- `show ppp multilink`
- `show ptp clock`
- `show ptp foreign-master-record`
- `show ptp parent`
- `show ptp port`
- `show ptp time-property`
- `show rep topology`

- [show xconnect](#)
- [signaling](#)
- [snmp-server enable traps ethernet cfm alarm](#)
- [snmp-server enable traps ethernet cfm cc](#)
- [snmp-server enable traps ethernet cfm crosscheck](#)
- [switch l2trust](#)
- [switchport backup](#)
- [switchport stacking-partner](#)
- [traceroute ethernet](#)
- [traceroute ethernet](#)
- [tunnel destination](#)
- [tunnel source](#)
- [xconnect](#)
- [xconnect logging redundancy](#)

# address-family ipv4 (BGP)

To enter address family or router scope address family configuration mode to configure a routing session using standard IP Version 4 address prefixes, use the **address-family ipv4** command in router scope configuration mode. To exit address family configuration mode and remove the IPv4 address family configuration from the running configuration, use the **no** form of this command.

## Syntax Available Under Router Scope Configuration Mode

**address-family ipv4 [mdt]**

**no address-family ipv4 [mdt]**

|                           |                                                                                                   |
|---------------------------|---------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>mdt</b> (Optional) Specifies an IPv4 multicast distribution tree (MDT) address family session. |
|---------------------------|---------------------------------------------------------------------------------------------------|

|                        |                                                |
|------------------------|------------------------------------------------|
| <b>Command Default</b> | IP Version 4 address prefixes are not enabled. |
|------------------------|------------------------------------------------|

|                      |                                                                                          |
|----------------------|------------------------------------------------------------------------------------------|
| <b>Command Modes</b> | Router configuration (config-router)<br>Router scope configuration (config-router-scope) |
|----------------------|------------------------------------------------------------------------------------------|

| <b>Command History</b> | <b>Release</b>           | <b>Modification</b>                                                                                                                                                                                 |
|------------------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | 12.0(5)T                 | This command was introduced. This command replaced the <b>match nlri</b> and <b>set nlri</b> commands.                                                                                              |
|                        | 12.0(28)S                | This command was integrated into Cisco IOS Release 12.0(28)S, and the <b>tunnel</b> keyword was added.                                                                                              |
|                        | 12.0(29)S                | The <b>mdt</b> keyword was added.                                                                                                                                                                   |
|                        | 12.0(30)S                | Support for the Cisco 12000 series Internet router was added.                                                                                                                                       |
|                        | 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                                     |
|                        | 12.2(31)SB2              | This command was integrated into Cisco IOS Release 12.2(31)SB2.                                                                                                                                     |
|                        | 12.2(33)SRB              | Support for the router scope configuration mode was added.                                                                                                                                          |
|                        | 12.2(33)SXH              | This command was integrated into Cisco IOS Release 12.2(33)SXH.                                                                                                                                     |
|                        | 12.2(33)SB               | This command was integrated into Cisco IOS Release 12.2(33)SB.                                                                                                                                      |
|                        | Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                       |
|                        | 12.4(20)T                | The <b>mdt</b> keyword was added.                                                                                                                                                                   |
|                        | 12.2(33)MRB              | This command was integrated into Cisco IOS Release 12.2(33)MRB. This command is only supported Router Scope Configuration Mode. The <b>multicast</b> and <b>unicast</b> keywords are not supported. |

**Usage Guidelines**

The **address-family ipv4** command replaces the **match nlri** and **set nlri** commands. The **address-family ipv4** command places the router in address family configuration mode (prompt: `config-router-af`), from which you can configure routing sessions that use standard IP Version 4 address prefixes. To leave address family configuration mode and return to router configuration mode, type **exit**.

The **mdt** keyword is used to enable the MDT SAFI under the IPv4 address family identifier. This SAFI is used to advertise tunnel endpoints for inter-AS multicast VPN peering sessions.

In Cisco IOS Release 12.2(33)SRB and later releases, the ability to use address family configuration under the router scope configuration mode was introduced. The scope hierarchy can be defined for BGP routing sessions and is required to support Multi-Topology Routing (MTR). To enter the router scope configuration mode, use the **scope** command, which can apply globally or for a specific VRF. When using the scope for a specific VRF, only the **unicast** keyword is available.

**Examples**

The following example places the router in address family configuration mode for the IP Version 4 address family:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4
Router(config-router-af)#
```

**MDT Example**

The following example shows how to configure a router to support an IPv4 MDT address-family session:

```
Router(config)# router bgp 45000
Router(config-router)# address-family ipv4 mdt
Router(config-router-af)#
```

**Router Scope Configuration Mode Example**

The following example shows how to configure the IPv4 address family under router scope configuration mode. In this example, the scope hierarchy is enabled globally. The router enters router scope address family configuration mode, and only multicast address prefixes for the IP Version 4 address family are specified:

```
Router(config)# router bgp 50000
Router(config-router)# scope global
Router(config-router-scope)# address-family ipv4 multicast
Router(config-router-scope-af)#
```

**Related Commands**

| Command                   | Description                                                   |
|---------------------------|---------------------------------------------------------------|
| <b>neighbor remote-as</b> | Adds an entry to the BGP or multiprotocol BGP neighbor table. |

## alarm (config-if-ecfm-mep mode)

To configure an alarm when fault alarms are enabled, use the **alarm** command in Ethernet connectivity fault management (CFM) interface configuration mode. To remove the configuration, use the **no** form of this command.

**alarm** {**delay** *mseconds* | **notification** {**all** | **error-xcon** | **mac-remote-error-xcon** | **none** | **remote-error-xcon** | **xcon**} | **reset** *mseconds*}

**no alarm** {**delay** | **notification** {**all** | **error-xcon** | **mac-remote-error-xcon** | **none** | **remote-error-xcon** | **xcon**} | **reset**}

### Syntax Description

|                              |                                                                                                                                                                                                                           |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>delay</b>                 | Sets a delay time value during which one or more defects must be present before a fault alarm is issued.                                                                                                                  |
| <i>mseconds</i>              | Integer from 2500 to 10000 that specifies the number of milliseconds for either a delay or a reset of an alarm.<br><br>The default is 2500 for the <b>delay</b> option. The default is 10000 for the <b>reset</b> option. |
| <b>notification</b>          | Sets the defects that are to be reported if fault alarms are enabled.                                                                                                                                                     |
| <b>all</b>                   | Reports all defects: DefRDI, DefMACStatus, DefRemote, DefError, and DefXcon.                                                                                                                                              |
| <b>error-xcon</b>            | Reports only DefError and DefXcon defects.                                                                                                                                                                                |
| <b>mac-remote-error-xcon</b> | Reports only DefMACStatus, DefRemote, DefError, and DefXcon (default) defects. This option is the default.                                                                                                                |
| <b>none</b>                  | No defects are reported.                                                                                                                                                                                                  |
| <b>remote-error-xcon</b>     | Reports only DefRemote, DefError, and DefXcon defects.                                                                                                                                                                    |
| <b>xcon</b>                  | Reports only DefXcon defects.                                                                                                                                                                                             |
| <b>reset</b>                 | Sets a reset time value that, after a fault alarm, no defects must be present before another fault alarm is enabled.                                                                                                      |

### Command Default

Alarms are disabled.

### Command Modes

Ethernet CFM interface configuration (config-if-ecfm-mep)

### Command History

| Release      | Modification                                                    |
|--------------|-----------------------------------------------------------------|
| 12.2(33)SX12 | This command was introduced.                                    |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

### Usage Guidelines

This command overrides the global **ethernet cfm alarm** command.

If a higher priority defect occurs after a lower priority defect has triggered an alarm but before the alarm has reset, immediately issue another fault alarm for the higher priority defect.

Output of the **show running all** command displays “alarm delay 2500” when the default value for the **delay** option is configured, “alarm mac-remote-error-xcon” when the default value for the **notification** option is configured, and “alarm reset 10000” when the default value for the **reset** option is configured.

### Examples

The following example shows how to set up notifications for all defects:

```
Router(config)# ethernet cfm domain test level 5
Router(config-ether-cfm)# service vlan-id 17 vlan 17
Router(config-ether-cfm)# exit
Router(config-if)# ethernet cfm mep domain test mpid 5 vlan 17
Router(config-if-ecfm-mep)# alarm notification all
Router(config-if-ecfm-mep)#
```

The following example shows how to set the time during which one or more defects must be present before a fault alarm is issued to 7000 milliseconds:

```
Router(config)# ethernet cfm domain test level 5
Router(config-ether-cfm)# service vlan-id 17 vlan 17
Router(config-ether-cfm)# exit
Router(config-if)# ethernet cfm mep domain test mpid 5 vlan 17
Router(config-if-ecfm-mep)# alarm delay 7000
```

### Related Commands

| Command                 | Description                                          |
|-------------------------|------------------------------------------------------|
| <b>show running all</b> | Shows the running configuration with default values. |



# atm ilmi-keepalive

To enable Interim Local Management Interface (ILMI) keepalives, use the **atm ilmi-keepalive** command in interface configuration mode. To disable ILMI keepalives, use the **no** form of this command.

**atm ilmi-keepalive** [*seconds*]

**no atm ilmi-keepalive** [*seconds*]

|                           |                                                                                                                                                      |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>seconds</i> (Optional) Number of seconds between keepalives. Values less than 3 seconds are rounded up to 3 seconds, and there is no upper limit. |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|

|                        |   |
|------------------------|---|
| <b>Command Default</b> | 3 |
|------------------------|---|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | Interface configuration |
|----------------------|-------------------------|

| Command History | Release     | Modification                                                                                                                                                                      |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 11.0        | This command was introduced.                                                                                                                                                      |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not provide support for DSL HWICs.                                                              |

**Examples** The following example enables ILMI keepalives for the ATM interface 1/0:

```
interface atm 1/0
 atm address-registration
 atm ilmi-keepalive
```

| Related Commands | Command                         | Description                                                                                |
|------------------|---------------------------------|--------------------------------------------------------------------------------------------|
|                  | <b>atm address-registration</b> | Enables the router to engage in address registration and callback functions with the ILMI. |

## atm vc-per-vp

To set the maximum number of virtual channel identifier (VCIs) to support per virtual path identifier (VPI), use the **atm vc-per-vp** interface configuration command. To restore the default value, use the **no** form of this command.

**atm vc-per-vp** *number*

**no atm vc-per-vp**

### Syntax Description

*number* Maximum number of VCIs to support per VPI. Valid values are:

- 16
- 128
- 256
- 1024
- 2048
- 4096
- 16384
- 65536

### Command Default

1024

### Command Modes

Interface configuration

### Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.0        | This command was introduced.                                                                                                                                                      |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not provide support for DSL HWICs.                                                              |

### Usage Guidelines

This command controls the memory allocation in the ATM Interface Processor (AIP), ATM port adapter, ATM network module, or network processor module (NPM) to deal with the VCI table. It defines the maximum number of VCIs to support per VPI; it does not bound the VCI numbers.

An invalid VCI causes a warning message to be displayed.

**Note**

Changing the value of the **atm vc-per-vp** command on one interface affects all of the interfaces on that network module.

Table 1 lists the possible VCI ranges and corresponding VPI ranges.

**Table 1** VCI and VPI Ranges for Cisco 2600 and 3600 Series with IMA

| VCI Range | VPI Range                         |
|-----------|-----------------------------------|
| 0–255     | 0–15, 64–79, 128–143, and 192–207 |
| 0–511     | 0–15, 64–79                       |
| 0–1023    | 0–15                              |

**Examples**

The following example sets the maximum number of VCIs per VPI to 512:

```
Router(config)# interface atm1/0
Router(config-if)# atm vc-per-vp 512
```

**Related Commands**

| Command    | Description                   |
|------------|-------------------------------|
| <b>pvc</b> | Configures the PVC interface. |

# backup delay

To specify how long a backup pseudowire (PW) virtual circuit (VC) should wait before resuming operation after the primary PW VC goes down, use the **backup delay** command in interface configuration mode or xconnect configuration mode. To return to the default so that as soon as the primary fails, the secondary is immediately brought up without delay, use the **no** form of this command.

**backup delay** *enable-delay* {*disable-delay* | **never**}

**no backup delay** *enable-delay* {*disable-delay* | **never**}

|                           |                      |                                                                                                                                                                        |
|---------------------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>enable-delay</i>  | Number of seconds that elapse after the primary PW VC goes down before the Cisco IOS software activates the secondary PW VC. The range is 0 to 180. The default is 0.  |
|                           | <i>disable-delay</i> | Number of seconds that elapse after the primary PW VC comes up before the Cisco IOS software deactivates the secondary PW VC. The range is 0 to 180. The default is 0. |
|                           | <b>never</b>         | The secondary PW VC does not fall back to the primary PW VC if the primary PW VC becomes available again, unless the secondary PW VC fails.                            |

|                        |                                                                                                                                                          |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Command Default</b> | If a failover occurs, the xconnect redundancy algorithm immediately switches over or falls back to the backup or primary member in the redundancy group. |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|

|                      |                                                   |
|----------------------|---------------------------------------------------|
| <b>Command Modes</b> | Interface configuration<br>Xconnect configuration |
|----------------------|---------------------------------------------------|

| <b>Command History</b> | Release      | Modification                                                     |
|------------------------|--------------|------------------------------------------------------------------|
|                        | 10.0         | This command was introduced.                                     |
|                        | 12.2(33)SRB1 | This command was integrated into Cisco IOS Release 12.2(33)SRB1. |
|                        | 12.4(19)MR2  | This command was integrated into Cisco IOS Release 12.4(19)MR2.  |
|                        | 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.  |

|                 |                                                                                                                                                                                                                           |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | The following example shows a Multiprotocol Label Switching (MPLS) xconnect with one redundant peer. After a switchover to the secondary VC occurs, there is no fallback to the primary VC unless the secondary VC fails. |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# exit
Router(config)# interface atm1/0
Router(config-if)# xconnect 10.0.0.1 50 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 50
Router(config-if-xconn)# backup delay 0 never
Router(config-if-xconn)# exit
```

```
Router(config-if)# exit
Router(config)# exit
```

The following example shows an MPLS xconnect with one redundant peer. The switchover does not begin unless the PW has been down for 3 seconds. After a switchover to the secondary VC occurs, there is no fallback to the primary until the primary VC has been reestablished and is up for 10 seconds.

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# exit
Router(config)# interface atm1/0
Router(config-if)# xconnect 10.0.0.1 50 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 50
Router(config-if-xconn)# backup delay 3 10
Router(config-if-xconn)# exit
Router(config-if)# exit
Router(config)# exit
```

**Related Commands**

| Command            | Description                              |
|--------------------|------------------------------------------|
| <b>backup peer</b> | Configures a redundant peer for a PW VC. |

# backup peer

To specify a redundant peer for a pseudowire (PW) virtual circuit (VC), use the **backup peer** command in interface configuration mode or xconnect configuration mode. To remove the redundant peer, use the **no** form of this command.

**backup peer** *peer-router-ip-addr* *vcid* [**pw-class** *pw-class-name*]

**no backup peer** *peer-router-ip-addr* *vcid*

## Syntax Description

|                            |                                                                                               |
|----------------------------|-----------------------------------------------------------------------------------------------|
| <i>peer-router-ip-addr</i> | IP address of the remote peer.                                                                |
| <i>vcid</i>                | The 32-bit identifier of the VC between the routers at each end of the layer control channel. |
| <b>pw-class</b>            | (Optional) PW type. If not specified, the PW type is inherited from the parent xconnect.      |
| <i>pw-class-name</i>       | (Optional) Name of the PW you created when you established the PW class.                      |

## Command Default

No redundant peer is established.

## Command Modes

Interface configuration  
Xconnect configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.0(31)S   | This command was introduced.                                    |
| 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.  |
| 12.4(11)T   | This command was integrated into Cisco IOS Release 12.4(11)T.   |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |
| 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

The combination of the *peer-router-ip-addr* and *vcid* arguments must be unique on the router.

## Examples

The following example shows an MPLS xconnect with one redundant peer:

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# exit
Router(config)# interface atm1/0
Router(config-if)# xconnect 10.0.0.1 100 pw-class mpls
```

```
Router(config-if-xconn)# backup peer 10.0.0.2 200
Router(config-if-xconn)# exit
Router(config-if)# exit
Router(config)# exit
```

The following example shows a backup peer configuration for an ATM interface:

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# exit
Router(config)# interface atm0/1
Router(config-if)# xconnect 10.0.0.2 1 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 100 pw-class mpls
Router(config-if-xconn)# exit
Router(config-if)# exit
Router(config)# exit
```

#### Related Commands

| Command             | Description                                                                                                  |
|---------------------|--------------------------------------------------------------------------------------------------------------|
| <b>backup delay</b> | Specifies how long the backup PW VC should wait before resuming operation after the primary PW VC goes down. |

## bandwidth (policy-map class)

To specify or modify the bandwidth allocated for a class belonging to a policy map, or to enable ATM overhead accounting, use the **bandwidth** command in policy-map class configuration mode. To remove the bandwidth specified for a class or disable ATM overhead accounting, use the **no** form of this command.

**bandwidth** { *bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage* }

**no bandwidth**

### Syntax Description

|                                            |                                                                                                                                                                              |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>bandwidth-kbps</i>                      | Amount of bandwidth, in kilobits per second (kbps), to be assigned to the class. The amount of bandwidth varies according to the interface and platform in use.              |
| <b>remaining percent</b> <i>percentage</i> | Percentage of guaranteed bandwidth based on a relative percent of available bandwidth. The percentage can be a number from 1 to 100.                                         |
| <b>percent</b> <i>percentage</i>           | Percentage of guaranteed bandwidth based on an absolute percent of available bandwidth to be set aside for the priority class. The percentage can be a number from 1 to 100. |

### Command Default

No bandwidth is specified.  
ATM overhead accounting is disabled.

### Command Modes

Policy-map class configuration (config-pmap-c)

### Command History

| Release     | Modification                                                                                                                                                           |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(5)T    | This command was introduced.                                                                                                                                           |
| 12.0(5)XE   | This command was integrated into Cisco IOS Release 12.0(5)XE and was implemented on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers.             |
| 12.0(7)T    | The <b>percent</b> keyword was added.                                                                                                                                  |
| 12.0(17)SL  | This command was introduced on the Cisco 10000 series router.                                                                                                          |
| 12.0(22)S   | Support for the <b>percent</b> keyword was added on the Cisco 10000 series router.                                                                                     |
| 12.0(23)SX  | Support for the <b>remaining percent</b> keyword was added on the Cisco 10000 series router.                                                                           |
| 12.1(5)T    | This command was implemented on VIP-enabled Cisco 7500 series routers.                                                                                                 |
| 12.2(2)T    | The <b>remaining percent</b> keyword was added.                                                                                                                        |
| 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                                                         |
| 12.2(31)SB  | This command was implemented on the Cisco 10000 series routers.                                                                                                        |
| 12.2(31)SB2 | This command was introduced on the PRE3 for the Cisco 10000 series router, and was enhanced for ATM overhead accounting on the Cisco 10000 series router for the PRE3. |



| Release                  | Modification                                                                                                                                                                      |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX                   | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(31)SB6              | This command was enhanced to specify an offset size when calculating ATM overhead and was implemented on the Cisco 10000 series router for the PRE3.                              |
| 12.2(33)SRC              | Support for the Cisco 7600 series router was added.                                                                                                                               |
| 12.2(33)SB               | Support for the Cisco 7300 series router was added.                                                                                                                               |
| 12.4(20)T                | Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).                                        |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers.                                                                                                                    |
| 12.4(20)MR               | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA              | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

## Usage Guidelines

### Configuring a Policy Map

Use the **bandwidth** command when you configure a policy map for a class defined by the **class-map** command. The **bandwidth** command specifies the bandwidth for traffic in that class. Class-based weighted fair queueing (CBWFQ) derives the weight for packets belonging to the class from the bandwidth allocated to the class. CBWFQ then uses the weight to ensure that the queue for the class is serviced fairly.

### Configuring Strict Priority with Bandwidth

You can configure only one class with strict priority. Other classes cannot have priority or bandwidth configuration. To configure minimum bandwidth for another class, use the **bandwidth remaining percent** command.

### Specifying Bandwidth as a Percentage

Besides specifying the amount of bandwidth in kilobits per second (kbps), you can specify bandwidth as a percentage of either the available bandwidth or the total bandwidth. During periods of congestion, the classes are serviced in proportion to their configured bandwidth percentages. The bandwidth percentage is based on the interface bandwidth or when used in a hierarchical policy. Available bandwidth is equal to the interface bandwidth minus the sum of all bandwidths reserved by the Resource Reservation Protocol (RSVP) feature, the IP RTP Priority feature, and the low latency queueing (LLQ) feature.



#### Note

It is important to remember that when the **bandwidth remaining percent** command is configured, hard bandwidth guarantees may not be provided and only relative bandwidths are assured. That is, class bandwidths are always proportional to the specified percentages of the interface bandwidth. When the link bandwidth is fixed, class bandwidth guarantees are in proportion to the configured percentages. If the link bandwidth is unknown or variable, the router cannot compute class bandwidth guarantees in kbps.

The router converts the specified bandwidth to the nearest multiple of 1/255 (ESR–PRE1) or 1/65,535 (ESR–PRE2) of the interface speed. Use the **show policy-map interface** command to display the actual bandwidth.

### Restrictions

The following restrictions apply to the **bandwidth** command:

- The amount of bandwidth configured should be large enough to also accommodate Layer 2 overhead.
- A policy map can have all the class bandwidths specified in kbps or all the class bandwidths specified in percentages, but not a mix of both in the same class. However, the unit for the **priority** command in the priority class can be different from the bandwidth unit of the nonpriority class.
- When the **bandwidth percent** command is configured, and a policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, the policy is removed from all interfaces to which it was successfully attached. This restriction does not apply to the **bandwidth remaining percent** command.

| Related Commands | Command                          | Description                                                                                                                                                                         |
|------------------|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>class (policy-map)</b>        | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.       |
|                  | <b>class-map</b>                 | Creates a class map to be used for matching packets to a specified class.                                                                                                           |
|                  | <b>max-reserved-bandwidth</b>    | Changes the percent of interface bandwidth allocated for CBWFQ, LLQ, and IP RTP Priority.                                                                                           |
|                  | <b>policy-map</b>                | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                        |
|                  | <b>priority</b>                  | Specifies the priority of a class of traffic belonging to a policy map.                                                                                                             |
|                  | <b>queue-limit</b>               | Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map.                                                               |
|                  | <b>show policy-map</b>           | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.                                                           |
|                  | <b>show policy-map interface</b> | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# bfd all-interfaces

To enable Bidirectional Forwarding Detection (BFD) for all interfaces participating in the routing process, use the **bfd all-interfaces** command in router configuration mode. To disable BFD for all interfaces, use the **no** form of this command.

- bfd all-interfaces**
- no bfd all-interfaces**

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is not enabled on the interfaces participating in the routing process.

Command Modes

Router configuration

Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(18)SXE | This command was introduced.                                    |
| 12.0(31)S   | This command was integrated into Cisco IOS Release 12.0(31)S.   |
| 12.4(4)T    | This command was integrated into Cisco IOS Release 12.4(4)T.    |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

Usage Guidelines

There are two methods to configure routing protocols to use BFD for failure detection. To enable BFD for all neighbors of a routing protocol, enter the **bfd all-interfaces** command in router configuration mode. If you do not want to enable BFD on all interfaces, enter the **bfd interface** command in router configuration mode.

Examples

The following example shows BFD enabled for all Intermediate System-to-Intermediate System (IS-IS) neighbors:

```
Router> enable
Router# configure terminal
Router(config)# router isis tag1
Router(config-router)# bfd all-interfaces
Router(config-router)# end
```

The following example shows BFD enabled for all Open Shortest Path First (OSPF) neighbors:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 123
Router(config-router)# bfd all-interfaces
Router(config-router)# end
```

| Related Commands | Command              | Description                                               |
|------------------|----------------------|-----------------------------------------------------------|
|                  | <b>bfd</b>           | Sets the baseline BFD session parameters on an interface. |
|                  | <b>bfd interface</b> | Enables BFD on a per-interface basis for a BFD peer.      |

# bfd interval

To set the baseline Bidirectional Forwarding Detection (BFD) session parameters on an interface, use the **bfd** command in interface configuration mode. To remove the baseline BFD session parameters, use the **no** form of this command.

**bfd interval** *milliseconds* **min\_rx** *milliseconds* **multiplier** *multiplier-value*

**no bfd interval** *milliseconds* **min\_rx** *milliseconds* **multiplier** *multiplier-value*

|                                           |                                                                                                                                                                                                                                                                                          |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b>                 | <b>interval</b> <i>milliseconds</i> Specifies the rate at which BFD control packets are sent to BFD peers. The configurable time period for the <i>milliseconds</i> argument is from 50 to 999 milliseconds (ms).                                                                        |
| <b>min_rx</b> <i>milliseconds</i>         | Specifies the rate at which BFD control packets are expected to be received from BFD peers. The configurable time period for the <i>milliseconds</i> argument is from 1 to 999 milliseconds (ms).                                                                                        |
| <b>multiplier</b> <i>multiplier-value</i> | Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The configurable value range for the <i>multiplier-value</i> argument is from 3 to 50. |

**Command Default** No baseline BFD session parameters are set.

**Command Modes** Interface configuration (config-if)

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                             |
|------------------------|----------------|-----------------------------------------------------------------|
|                        | 12.2(18)SXE    | This command was introduced.                                    |
|                        | 12.0(31)S      | This command was integrated into Cisco IOS Release 12.0(31)S.   |
|                        | 12.4(4)T       | This command was integrated into Cisco IOS Release 12.4(4)T.    |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
|                        | 12.2(33)SB     | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Examples** The following example shows the BFD session parameters set for Fast Ethernet interface 3/0:

```
Router> enable
Router# configure terminal
Router(config)# interface vlan1
Router(config-if)# bfd interval 50 min_rx 3 multiplier 3
Router(config-if)# end
```

| Related Commands | Command                   | Description                                              |
|------------------|---------------------------|----------------------------------------------------------|
|                  | <b>bfd all-interfaces</b> | Enables BFD for all interfaces for a BFD peer.           |
|                  | <b>bfd interface</b>      | Enables BFD on a per-interface basis for a BFD peer.     |
|                  | <b>ip ospf bfd</b>        | Enables BFD on a specific interface configured for OSPF. |

# cbr

To configure the constant bit rate (CBR) for the ATM circuit emulation service (CES) for an ATM permanent virtual circuit (PVC), use the **cbr** command in the appropriate configuration mode. To restore the default, use the **no** form of this command.

**cbr** *rate*

**no cbr** *rate*

## Syntax Description

|             |                                                                                                     |
|-------------|-----------------------------------------------------------------------------------------------------|
| <i>rate</i> | Constant bit rate (also known as the average cell rate) for ATM CES. Valid values are 32–1920 kbps. |
|-------------|-----------------------------------------------------------------------------------------------------|

## Command Default

The CBR is not configured.

## Command Modes

Interface-ATM-VC configuration (for ATM PVCs and SVCs)  
PVC range configuration (for an ATM PVC range)  
PVC-in-range configuration (for an individual PVC within a PVC range)  
ATM PVP configuration

## Command History

| Release                  | Modification                                                                                                                                                                      |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0                     | This command was introduced for the ATM CES on the Cisco MC3810.                                                                                                                  |
| 12.1(5)T                 | This command was made available in PVC range and PVC-in-range configuration modes.                                                                                                |
| 12.2(5)                  | Support was added for the PA-A3 port adapter on the Cisco 7200 series routers.                                                                                                    |
| 12.2(7)                  | Support was added for the PA-A3 port adapter on the Cisco 7500 series routers.                                                                                                    |
| 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX                   | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.3 | This command was made available in ATM PVP configuration mode.                                                                                                                    |
| 12.4(20)MR               | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA              | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

## Examples

The following example configures the constant bit rate on ATM PVC 20:

```
pvc 20
  cbr 56
```



| Related Commands | Command    | Description                                                                                                                              |
|------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>pvc</b> | Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters interface-ATM-VC configuration mode. |

# cdp enable

To enable Cisco Discovery Protocol (CDP) on an interface, use the **cdp enable** command in interface configuration mode. To disable CDP on an interface, use the **no** form of this command.

**cdp enable**

**no cdp enable**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Enabled at the global level and on all supported interfaces.

## Command Modes

Interface configuration

## Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.3        | This command was introduced.                                                                                                                                                      |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2.                                                                                                                   |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

## Usage Guidelines

CDP is enabled by default at the global level and on each supported interface in order to send or receive CDP information. However, some interfaces, such as ATM interfaces, do not support CDP.



### Note

The **cdp enable**, **cdp timer**, and **cdp run** commands affect the operation of the IP on demand routing feature (that is, the **router odr** global configuration command). For more information on the **router odr** command, see the “On-Demand Routing Commands” chapter in the *Cisco IOS Command Reference, Volume 2 of 3: Routing Protocols* document.

## Examples

In the following example, CDP is disabled on the Ethernet 0 interface only:

```
Router# show cdp
Global CDP information
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
Router# config terminal
Router(config)# interface ethernet 0
Router(config-if)# no cdp enable
```

| Related Commands | Command           | Description                                                   |
|------------------|-------------------|---------------------------------------------------------------|
|                  | <b>cdp run</b>    | Reenables CDP on a Cisco device.                              |
|                  | <b>cdp timer</b>  | Specifies how often the Cisco IOS software sends CDP updates. |
|                  | <b>router odr</b> | Enables on-demand routing on a hub router.                    |

# cem-group

To create a circuit emulation (CEM) channel from one or more time slots of a T1 or E1 line, use the **cem-group** command in controller configuration mode. To remove a CEM group and release the associated time slots, use the **no** form of this command.

**cem-group** *group-number* {**unframed** | **timeslots** *time-slot-range*}

**no cem-group** *group-number*

## Syntax Description

|                        |                                                                                                                                                                                                      |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>group-number</i>    | CEM identifier to be used for this group of time slots: <ul style="list-style-type: none"> <li>For T1 ports, the range is from 0 to 23.</li> <li>For E1 ports, the range is from 0 to 30.</li> </ul> |
| <b>unframed</b>        | Specifies that a single CEM channel is being created, including all time slots, without specifying the framing structure of the line.                                                                |
| <b>timeslots</b>       | Specifies that a list of time slots is to be used as specified by the <i>time-slot-range</i> argument.                                                                                               |
| <i>time-slot-range</i> | Specifies the time slots to be included in the CEM channel. The list of time slots may include commas and hyphens with no spaces between the numbers.                                                |

## Command Default

No CEM groups are defined.

## Command Modes

Controller configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.3(7)T    | This command was introduced.                                    |
| 12.4(12)MR2 | This command was integrated into Cisco IOS Release 12.4(12)MR2. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

Use this command to create CEM channels on the T1 or E1 port.

## Examples

The following example shows how to create a CEM channel:

### SATOP

```
Router# config t
Router(config)# controller e1 0/0
Router(config-controller)# cem-group 0 unframed
Router(config-controller)# exit
Router(config)# interface cem 0/0
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
```

```
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

### CESoPSN

```
Router# config t
Router(config)# controller el 0/1
Router(config-controller)# cem-group 0 timeslots 1-31
Router(config-controller)# exit
Router(config)# interface cem 0/1
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

#### Related Commands

| Command    | Description                                  |
|------------|----------------------------------------------|
| <b>cem</b> | Enters circuit emulation configuration mode. |

# class (policy-map)

To specify the name of the class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy, use the **class** command in policy-map configuration mode. To remove a class from the policy map, use the **no** form of this command.

**class** {*class-name* | **class-default**}

**no class** {*class-name* | **class-default**}

## Syntax Description

|                      |                                                                                                                                                                                |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>class-name</i>    | Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map. |
| <b>class-default</b> | Specifies the default class so that you can configure or modify its policy.                                                                                                    |

## Command Default

No class is specified.

## Command Modes

Policy-map configuration (config-pmap)

## Command History

| Release                  | Modification                                                                                                                                                                                                       |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(5)T                 | This command was introduced.                                                                                                                                                                                       |
| 12.0(5)XE                | This command was integrated into Cisco IOS Release 12.0(5)XE.                                                                                                                                                      |
| 12.0(7)S                 | This command was integrated into Cisco IOS Release 12.0(7)S.                                                                                                                                                       |
| 12.1(1)E                 | This command was integrated into Cisco IOS Release 12.1(1)E.                                                                                                                                                       |
| 12.2(14)SX               | Support for this command was introduced on Cisco 7600 routers.                                                                                                                                                     |
| 12.2(17d)SXB             | This command was implemented on the Cisco 7600 router and integrated into Cisco IOS Release 12.2(17d)SXB.                                                                                                          |
| 12.2(18)SXE              | The <b>class-default</b> keyword was added to the Cisco 7600 router.                                                                                                                                               |
| 12.4(4)T                 | The <b>insert-before</b> <i>class-name</i> option was added.                                                                                                                                                       |
| 12.2(28)SB               | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                                                                                                     |
| 12.2(31)SB2              | This command was introduced on the PRE3 for the Cisco 10000 series router.                                                                                                                                         |
| 12.2(18)ZY               | The <b>insert-before</b> <i>class-name</i> option was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA). |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers. The <b>fragment</b> <i>fragment-class-name</i> and <b>service-fragment</b> <i>fragment-class-name</i> options were introduced.                      |

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR. This release does not support the <b>fragment</b> , <b>insert-before</b> , or <b>service-fragment</b> parameters.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not support the <b>fragment</b> , <b>insert-before</b> , or <b>service-fragment</b> parameters. |

## Usage Guidelines

### Policy Map Configuration Mode

Within a policy map, the **class** (policy-map) command can be used to specify the name of the class whose policy you want to create or change. First, the policy map must be identified.

To identify the policy map (and enter the required policy-map configuration mode), use the **policy-map** command before you use the **class** (policy-map) command. After you specify a policy map, you can configure policy for new classes or modify the policy for any existing classes in that policy map.

### Class Characteristics

The class name that you specify in the policy map ties the characteristics for that class—that is, its policy—to the class map and its match criteria, as configured using the **class-map** command.

When you configure policy for a class and specify its bandwidth and attach the policy map to an interface, class-based weighted fair queueing (CBWFQ) determines if the bandwidth requirement of the class can be satisfied. If so, CBWFQ allocates a queue for the bandwidth requirement.

When a class is removed, available bandwidth for the interface is incremented by the amount previously allocated to the class.

The maximum number of classes that you can configure for a router—and, therefore, within a policy map—is 64.

### Predefined Default Class

The **class-default** keyword is used to specify the predefined default class called class-default. The class-default class is the class to which traffic is directed if that traffic does not match any of the match criteria in the configured class maps.

### Tail Drop or WRED

You can define a class policy to use either tail drop by using the **queue-limit** command or Weighted Random Early Detection (WRED) by using the **random-detect** command. When using either tail drop or WRED, note the following points:

- The **queue-limit** and **random-detect** commands cannot be used in the same class policy, but they can be used in two class policies in the same policy map.
- You can configure the **bandwidth** command when either the **queue-limit** command or the **random-detect** command is configured in a class policy. The **bandwidth** command specifies the amount of bandwidth allocated for the class.
- For the predefined default class, you can configure the **fair-queue** (class-default) command. The **fair-queue** command specifies the number of dynamic queues for the default class. The **fair-queue** command can be used in the same class policy as either the **queue-limit** command or the **random-detect** command. It cannot be used with the **bandwidth** command.

## Fragments

A default traffic class is marked as a fragment within a policy map class statement using the **fragment** keyword. Multiple fragments can then be classified collectively in a separate policy map that is created using the **service-fragment** keyword. When fragments are used, default traffic classes marked as fragments have QoS applied separately from the non-default traffic classes.

When using fragments, note the following guidelines:

- Only default traffic classes can be marked as fragments.
- The **fragment** *fragment-class-name* option within a default class statement marks that default class as a fragment.
- The **service-fragment** *fragment-class-name* option when defining a class in a policy map is used to specify a class of traffic within the Modular QoS CLI that contains all fragments sharing the same *fragment-class-name*.
- Fragments can only be used within the same physical interface. Policy maps with fragments sharing the same *fragment-class-name* on different interfaces cannot be classified collectively using a class with the **service-fragment** *fragment-class-name* option.

## Examples

The following example configures three class policies included in the policy map called policy1. Class1 specifies policy for traffic that matches access control list 136. Class2 specifies policy for traffic with a CoS value of 2. The third class is the default class to which packets that do not satisfy configured match criteria are directed.

```
! The following commands create class-maps class1 and class2
! and define their match criteria:
```

```
class-map class1
  match access-group 136
class-map class2
  match cos 2
```

```
! The following commands create the policy map, which is defined to contain policy
! specification for class1, class2, and the default class:
policy-map policy1
```

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40

Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# random-detect exponential-weighting-constant 10

Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 16
Router(config-pmap-c)# queue-limit 20
```



| Related Commands | Command                                             | Description                                                                                                                   |
|------------------|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>bandwidth (policy-map class)</b>                 | Specifies or modifies the bandwidth allocated for a class belonging to a policy map.                                          |
|                  | <b>class-map</b>                                    | Creates a class map to be used for matching packets to a specified class.                                                     |
|                  | <b>fair-queue (class-default)</b>                   | Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy. |
|                  | <b>policy-map</b>                                   | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                  |
|                  | <b>queue-limit</b>                                  | Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map.         |
|                  | <b>random-detect (interface)</b>                    | Enables WRED or DWRED.                                                                                                        |
|                  | <b>random-detect exponential-weighting-constant</b> | Configures the WRED and DWRED exponential weight factor for the average queue size calculation.                               |
|                  | <b>random-detect precedence</b>                     | Configures WRED and DWRED parameters for a particular IP Precedence.                                                          |

# class cem

To configure CEM interface parameters in a class that is applied to CEM interfaces together, use the **class cem** command in global configuration mode. This command works in the same manner for CEM interfaces as the **pseudowire-class** command does for xconnect.

**class cem** *class-name*

## Syntax Description

|                   |                                               |
|-------------------|-----------------------------------------------|
| <i>class-name</i> | The name of a CEM interface parameters class. |
|-------------------|-----------------------------------------------|

## Command Default

None.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(12)MR2 | This command was incorporated.                                  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

The **class cem** command allows you to configure CEM interface parameters in a class that is applied to CEM interfaces together. A **class cem** command includes the following configuration settings:

- **de jitter-buffer** *de jitter-in-ms*
- **idle-pattern** *8-bit-idle-pattern*
- **payload-size** *payload-size-in-ms*



### Note

You can improve the performance of packet reordering on TDM/PWE connections by using the increasing the size of the de jitter buffer using the **de jitter-buffer** parameter.

## Examples

The following example shows how to configure CEM interface parameters:

```
Router# config t
Router(config)# class cem mycemclass
Router(config-cem-class)# de jitter-buffer 10
Router(config-cem-class)# sample-rate 32
Router(config-cem-class)# exit
Router(config)# interface cem 0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# cem class mycemclass
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

| Related Commands | Command                | Description                                                                                                                               |
|------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>cem</b>             | Enters circuit emulation configuration mode.                                                                                              |
|                  | <b>dejitter-buffer</b> | Specifies the size of the dejitter buffer used for network jitter in CEM configuration mode.                                              |
|                  | <b>idle-pattern</b>    | Specifies the data pattern to transmit on the T1/E1 line when missing packets are detected on the PWE3 circuit in CEM configuration mode. |
|                  | <b>sample-rate</b>     | Specifies in milliseconds the rate hardware samples the data on the attached circuit in CEM circuit configuration mode.                   |

# class-map

To create a class map to be used for matching packets to a specified class, use the **class-map** command in global configuration mode. To remove an existing class map from the router, use the **no** form of this command. The **class-map** command enters class-map configuration mode in which you can enter one of the **match** commands to configure the match criteria for this class.

**class map** [**match-all** | **match-any**] *class-map-name*

**no class map** [**match-all** | **match-any**] *class-map-name*

|                           |                       |                                                                                                                                                                                                                                                                                                                                 |
|---------------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>match-all</b>      | (Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under the class map using a logical AND function; a match requires that all statements be true. If you do not specify the <b>match-all</b> or <b>match-any</b> keyword, the default keyword is <b>match-all</b> .        |
|                           | <b>match-any</b>      | (Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map using a logical OR function; a match requires that one of the statements be true. If you do not specify the <b>match-any</b> or <b>match-all</b> keyword, the default keyword is <b>match-all</b> . |
|                           | <i>class-map-name</i> | Name of the class for the class map. The name can be a maximum of 40 alphanumeric characters. The class name is used for both the class map and to configure a policy for the class in the policy map.                                                                                                                          |

**Command Default** No class map is configured by default.

**Command Modes** Global configuration (config)

| <b>Command History</b> | Release      | Modification                                                                                                                                                                                                  |
|------------------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | 12.0(5)T     | This command was introduced.                                                                                                                                                                                  |
|                        | 12.0(5)XE    | This command was integrated into Cisco IOS Release 12.0(5)XE.                                                                                                                                                 |
|                        | 12.0(7)S     | This command was integrated into Cisco IOS Release 12.0(7)S.                                                                                                                                                  |
|                        | 12.1(1)E     | This command was integrated into Cisco IOS Release 12.1(1)E.                                                                                                                                                  |
|                        | 12.2(14)SX   | Support for this command was introduced on Cisco 7600 series routers.                                                                                                                                         |
|                        | 12.2(17d)SXB | This command was implemented on the Cisco 7600 series routers and integrated into Cisco IOS Release 12.2(17d)SXB.                                                                                             |
|                        | 12.2(33)SRA  | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                                               |
|                        | 12.4(4)T     | The <b>type stack</b> and <b>type access-control</b> keywords were added to support FPM. The <b>type port-filter</b> and <b>type queue-threshold</b> keywords were added to support Control Plane Protection. |
|                        | 12.4(6)T     | The <b>type logging</b> keyword was added to support control plane packet logging.                                                                                                                            |

| Release                  | Modification                                                                                                                                                                                                                   |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(18)ZY               | The <b>type stack</b> and <b>type access-control</b> keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA) |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers.                                                                                                                                                                 |
| 12.4(20)MR               | This command was integrated into Cisco IOS Release 12.4(20)MR. This release does not support the <b>stack</b> , <b>access-control</b> , <b>logging</b> , <b>port-filter</b> , and <b>queue-threshold</b> parameters.           |
| 12.2(33)MRA              | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not support the <b>stack</b> , <b>access-control</b> , <b>logging</b> , <b>port-filter</b> , and <b>queue-threshold</b> parameters.          |

### Usage Guidelines

Use the **class-map** command to specify the class that you create or modify to meet the class-map match criteria. This command enters class-map configuration mode in which you can enter one of the **match** commands to configure the match criteria for this class. Packets that arrive at either the input interface or the output interface (determined by how the **service-policy** command is configured) are checked against the match criteria configured for a class map to determine if the packets belong to that class.

When configuring a class map, you can use one or more **match** commands to specify match criteria. For example, you can use the **match access-group** command, the **match protocol** command, or the **match input-interface** command. The **match** commands vary according to the Cisco IOS release. For more information about match criteria and **match** commands, see the “Modular Quality of Service Command-Line Interface (CLI) (MQC)” chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

### Examples

The following example specifies class101 as the name of a class, and it defines a class map for this class. The class called class101 specifies policy for traffic that matches access control list 101.

```
Router(config)# class-map class101
Router(config-cmap)# match access-group 101
```

The following example shows how to access the **class-map** commands and subcommands, configure a class map named ipp5, and enter a match statement for IP precedence 5:

```
Router(config)# class-map ipp5
Router(config-cmap)# match ip precedence 5
```

### Related Commands

| Command                    | Description                                                                                                                                                                   |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>class (policy-map)</b>  | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |
| <b>class class-default</b> | Specifies the default class for a service policy map.                                                                                                                         |
| <b>match (class-map)</b>   | Configures the match criteria for a class map on the basis of port filter and/or protocol queue policies.                                                                     |
| <b>match access-group</b>  | Configures the match criteria for a class map on the basis of the specified ACL.                                                                                              |

| Command                          | Description                                                                                                                                                    |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>match input-interface</b>     | Configures a class map to use the specified input interface as a match criterion.                                                                              |
| <b>match ip dscp</b>             | Identifies one or more DSCP, AF, and CS values as a match criterion                                                                                            |
| <b>match mpls experimental</b>   | Configures a class map to use the specified EXP field value as a match criterion.                                                                              |
| <b>match protocol</b>            | Configures the match criteria for a class map on the basis of the specified protocol.                                                                          |
| <b>policy-map</b>                | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                   |
| <b>service-policy</b>            | Attaches a policy map to an input interface or virtual circuit (VC) or to an output interface or VC to be used as the service policy for that interface or VC. |
| <b>show class-map</b>            | Displays class-map information.                                                                                                                                |
| <b>show policy-map interface</b> | Displays the statistics and the configurations of the input and output policies that are attached to an interface.                                             |

# class-map type control

To create an Intelligent Services Gateway (ISG) control class map, which defines the conditions under which the actions of a control policy map are executed, use the **class-map type control** command in global configuration mode. To remove a control class map, use the **no** form of this command.

**class-map type control** [**match-all** | **match-any** | **match-none**] *class-map-name*

**no class-map type control** [**match-all** | **match-any** | **match-none**] *class-map-name*

## Syntax Description

|                       |                                                                                                |
|-----------------------|------------------------------------------------------------------------------------------------|
| <b>match-all</b>      | (Optional) Class map evaluates true if all of the conditions in the class map evaluates true.  |
| <b>match-any</b>      | (Optional) Class map evaluates true if any of the conditions in the class map evaluates true.  |
| <b>match-none</b>     | (Optional) Class map evaluates true if none of the conditions in the class map evaluates true. |
| <i>class-map-name</i> | Name of the class map.                                                                         |

## Command Default

A control class map is not created.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(28)SB  | This command was introduced.                                    |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

A control class map specifies conditions that must be met for a control policy to be activated, and, optionally, the event that causes the class to be evaluated. A control class map can contain multiple conditions, each of which is evaluated as either true or false. Use the **match-any**, **match-all**, and **match-none** keywords to specify which, if any, conditions must be true before the control policy is executed.

A control policy map, which is configured with the **policy-map type control** command, contains one or more control policy rules. A control policy rule associates a control class map with one or more actions. Use the **class type control** command to associate a control class map with a control policy map.

## Examples

The following example shows how to configure a control policy in which virtual private dial-up network (VPDN) forwarding is applied to anyone dialing in from "xyz.com":

```
class-map type control match-all MY-FORWARDED-USERS
match unauthenticated-domain "xyz.com"
!
```

**class-map type control**

```
policy-map type control MY-POLICY
  class type control MY-FORWARDED-USERS event session-start
    1 apply identifier nas-port
    2 service local
!
interface Dialer1
  service-policy type control MY-POLICY
```

**Related Commands**

| Command                        | Description                                                                                 |
|--------------------------------|---------------------------------------------------------------------------------------------|
| <b>class type control</b>      | Specifies a control class for which actions may be configured in an ISG control policy map. |
| <b>policy-map type control</b> | Creates or modifies a control policy map, which defines an ISG control policy.              |



# class-map type traffic

To create or modify a traffic class map, which is used for matching packets to a specified Intelligent Services Gateway (ISG) traffic class, use the **class-map type traffic** command in global configuration mode. To remove a traffic class map, use the **no** form of this command.

**class-map type traffic match-any** *class-map-name*

**no class-map type traffic match-any** *class-map-name*

## Syntax Description

|                       |                                                                                                             |
|-----------------------|-------------------------------------------------------------------------------------------------------------|
| <b>match-any</b>      | Indicates that packets must meet one of the match criteria in order to be considered a member of the class. |
| <i>class-map-name</i> | Name of the class map.                                                                                      |

## Command Default

A traffic class map is not created.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(28)SB  | This command was introduced.                                    |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

Use the **class-map type traffic** command to specify the name of the ISG traffic class for which you want to create or modify traffic class map match criteria. Use of the **class-map type traffic** command enables traffic class-map configuration mode, in which you can enter match commands to configure the match criteria for this class. Packets are checked against the match criteria configured for a class map to determine if the packet belongs to that traffic class.

ISG traffic classes allow subscriber session traffic to be subclassified so that ISG features can be applied to constituent flows. Traffic policies, which define the handling of data packets, contain a traffic class and one or more features.

Once a traffic class map has been defined, use the **class type traffic** command to associate the traffic class map with a service policy map. A service can contain one traffic class, and the default class.

## Examples

The following example shows the configuration of a traffic class map called “CLASS-ACL-101”. The class map is defined so that input traffic matching access list 101 matches the class. The traffic class map is then referenced in service policy map “mp3”.

```
class-map type traffic CLASS-ACL-101
  match access-group input 101
!
policy-map type service mp3
  class type traffic CLASS-ACL-101
```

**class-map type traffic**

```
authentication method-list cp-mlist
accounting method-list cp-mlist
prepaid conf-prepaid
```

**Related Commands**

| Command                         | Description                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>class type traffic</b>       | Specifies a named traffic class whose policy you want to create or change or specifies the default traffic class in order to configure its policy. |
| <b>match access-group (ISG)</b> | Configures the match criteria for a class map on the basis of the specified access control list (ACL).                                             |

# clear ethernet cfm errors

To clear continuity check error conditions logged on a device, use the **clear ethernet cfm errors** command in privileged EXEC mode.



## Note

Release 12.2(33)MRA supports the Draft 1.0 version of Ethernet CFM; it does not support the IEEE 802.1ag-2007 version.

### Cisco pre-Standard Connectivity Fault Management Draft 1.0 (CFM D1)

**clear ethernet cfm errors** [**domain** *domain-name* | **level** *level-id*]

### CFM IEEE 802.1ag Standard (CFM IEEE)

**clear ethernet cfm errors** [**domain-id** {*mac-address* *domain-number* | *domain-name* | **dns** *dns-name* | **null**}] [**service** {*ma-name* | *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*}]

## Syntax Description

|                      |                                                                                  |
|----------------------|----------------------------------------------------------------------------------|
| <b>domain</b>        | (Optional) Clears errors for a maintenance domain.                               |
| <i>domain-name</i>   | (Optional) String of a maximum of 154 characters.                                |
| <b>level</b>         | (Optional) Clears errors for a maintenance level.                                |
| <i>level-id</i>      | (Optional) Integer in the range of 0 to 7 that identifies the maintenance level. |
| <b>domain-id</b>     | (Optional) Clears errors by domain ID.                                           |
| <i>mac-address</i>   | (Optional) MAC address of the maintenance domain.                                |
| <i>domain-number</i> | (Optional) Integer in the range of 0 to 65535.                                   |
| <b>dns</b>           | (Optional) Specifies a domain name service (DNS).                                |
| <i>dns-name</i>      | (Optional) String of a maximum of 43 characters.                                 |
| <b>null</b>          | (Optional) Indicates there is not a domain name.                                 |
| <b>service</b>       | (Optional) Specifies a maintenance association within the domain.                |
| <i>ma-name</i>       | (Optional) String that identifies the maintenance association.                   |
| <i>ma-num</i>        | (Optional) Integer that identifies the maintenance association.                  |
| <b>vlan-id</b>       | (Optional) Specifies a VLAN.                                                     |
| <i>vlan-id</i>       | (Optional) Integer from 1 to 4094 that identifies the VLAN.                      |
| <b>vpn-id</b>        | (Optional) Specifies a virtual private network (VPN).                            |
| <i>vpn-id</i>        | (Optional) Integer from 1 to 32767 that identifies the VPN.                      |

## Command Default

The error database is unchanged; existing entries remain in the database.

## Command Modes

Privileged EXEC (#)

**Command History**

| Release      | Modification                                                     |
|--------------|------------------------------------------------------------------|
| 12.2(33)SRA  | This command was introduced.                                     |
| 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T.    |
| 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.  |
| 12.2(33)SXI2 | This command was integrated into Cisco IOS Release 12.2(33)SXI2. |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.  |

**Usage Guidelines**

Use the **clear ethernet cfm errors** command to purge error database entries that are not needed and when you want to work with a cleared database. Also, use this command with a specified domain if you want to clear errors for that domain.

In CFM IEEE, if a domain name has more than 43 characters, a warning message is displayed notifying that the maintenance domain ID (MDID) is truncated to 43 characters in continuity check messages (CCMs) if “id <fmt> <MDID>” is not configured.

**Examples**

The following example shows a **clear ethernet cfm errors** command for errors at maintenance level 3. No output is generated when this command is issued.

```
Router# clear ethernet cfm errors level 3
```

The following example shows how to clear errors for a DNS on VLAN 17. No output is generated when this command is issued.

```
Router# clear ethernet cfm errors domain-id dns Service10 service vlan-id 17
```

**Related Commands**

| Command                         | Description                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>show ethernet cfm errors</b> | Displays CFM continuity check error conditions logged on a device since it was last reset or since the log was last cleared. |

# clear ethernet cfm maintenance-points remote

To purge the contents of the continuity check database, use the **clear ethernet cfm maintenance-points remote** command in privileged EXEC mode.



## Note

Release 12.2(33)MRA supports the Draft 1.0 version of Ethernet CFM; it does not support the IEEE 802.1ag-2007 version.

### Cisco pre-Standard Connectivity Fault Management Draft 1.0 (CFM D1)

**clear ethernet cfm maintenance-points remote** [**domain** *domain-name* | **level** *level-id*]

### CFM IEEE 802.1ag Standard (CFM IEEE)

**clear ethernet cfm maintenance-points remote** [**domain** *domain-name*]

## Syntax Description

|                    |                                                                                  |
|--------------------|----------------------------------------------------------------------------------|
| <b>domain</b>      | (Optional) Indicates that a maintenance domain is specified.                     |
| <i>domain-name</i> | (Optional) String of a maximum of 154 characters that identifies the domain.     |
| <b>level</b>       | (Optional) Indicates that a maintenance level is specified.                      |
|                    | <b>Note</b> This keyword is not available in CFM IEEE.                           |
| <i>level-id</i>    | (Optional) Integer in the range of 0 to 7 that identifies the maintenance level. |
|                    | <b>Note</b> This argument is not available in CFM IEEE.                          |

## Command Default

The continuity check database is unchanged; existing entries remain in the database.

## Command Modes

Privileged EXEC (#)

## Command History

| Release      | Modification                                                     |
|--------------|------------------------------------------------------------------|
| 12.2(33)SRA  | This command was introduced.                                     |
| 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T.    |
| 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.  |
| 12.2(33)SXI2 | This command was integrated into Cisco IOS Release 12.2(33)SXI2. |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.  |

## Usage Guidelines

Use this command to clear the entire continuity check database or clear the database for a specific domain or level. When a domain is specified, only entries for that domain are purged. When a level is specified, entries for all domains at that level are purged.

If a maintenance domain is not specified, the entire continuity check database is cleared.

In CFM IEEE, the **level** keyword and *level-id* argument are not supported. Also, if a domain name has more than 43 characters, a warning message is displayed notifying that the maintenance domain ID (MDID) is truncated to 43 characters in continuity check messages (CCMs) if “id <fmt> <MDID>” is not configured.

---

**Examples**

The following example shows a **clear ethernet cfm maintenance-points remote** command. No output is generated when this command is issued.

```
Router# clear ethernet cfm maintenance-points remote
```

---

**Related Commands**

| Command                                            | Description                                                                            |
|----------------------------------------------------|----------------------------------------------------------------------------------------|
| <b>show ethernet cfm maintenance-points remote</b> | Displays information about remote maintenance points in the continuity check database. |

# clear ethernet cfm statistics

To clear a maintenance endpoint (MEP) or server maintenance endpoint (SMEP) out of the Alarm Indication Signal (AIS) defect condition, use the **clear ethernet cfm ais** command in privileged EXEC mode.

**clear ethernet cfm statistics** [**mpid** *mpid-id*]

## Syntax Description

|                |                                                                           |
|----------------|---------------------------------------------------------------------------|
| <b>mpid</b>    | (optional) Indicates that a maintenance point ID (MPID) is specified.     |
| <i>mpid-id</i> | (optional) An integer in the range of 1 to 8191 that identifies the MPID. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release      | Modification                                                    |
|--------------|-----------------------------------------------------------------|
| 12.2(33)SX12 | This command was introduced.                                    |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

If a MEP does not exit the AIS state when all errors are resolved, use the **clear ethernet cfm ais** command with the **domain** and **mpid** keywords to clear the AIS defect condition. If a SMEP does not exit the AIS state when all errors are resolved, use the **clear ethernet cfm ais** command with the **link-status interface** keywords to clear the AIS defect condition.

## Examples

The following example shows how to clear connectivity fault management (CFM) statistics from a SMEP of an AIS defect condition:

```
Router# clear ethernet cfm statistics mpid 800
```

## Related Commandss

| Command                       | Description                                           |
|-------------------------------|-------------------------------------------------------|
| <b>clear ethernet cfm ais</b> | Clears a MEP or SMEP out of the AIS defect condition. |

# clear ethernet cfm traceroute-cache

To remove the contents of the traceroute cache, use the **clear ethernet cfm traceroute-cache** command in privileged EXEC mode.

## clear ethernet cfm traceroute-cache

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC (#)

### Command History

| Release      | Modification                                                     |
|--------------|------------------------------------------------------------------|
| 12.2(33)SRA  | This command was introduced.                                     |
| 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T.    |
| 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.  |
| 12.2(33)SXI2 | This command was integrated into Cisco IOS Release 12.2(33)SXI2. |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.  |

### Usage Guidelines

Use the **clear ethernet cfm traceroute-cache** command to remove traceroute cache entries from previous traceroute operations issued on the device. This command also provides visibility into maintenance intermediate points and maintenance end points of a domain as they were recorded when the operation was performed.

### Examples

The following example shows the **clear ethernet cfm traceroute-cache** command:

```
Router# clear ethernet cfm traceroute-cache
```

### Related Commands

| Command                                   | Description                                                               |
|-------------------------------------------|---------------------------------------------------------------------------|
| <b>ethernet cfm traceroute cache</b>      | Enables caching of Ethernet CFM data learned through traceroute messages. |
| <b>show ethernet cfm traceroute-cache</b> | Displays the contents of the traceroute cache.                            |



# clock update-calendar

To perform a one-time update of the hardware clock (calendar) from the software clock, use the clock update-calendar command in user EXEC or privileged EXEC mode.

## clock update-calendar

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC  
Privileged EXEC

| Command History | Release     | Modification                                                                                                                                                                      |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 10.0        | This command was introduced.                                                                                                                                                      |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

**Usage Guidelines** Some platforms have a hardware clock (calendar) in addition to a software clock. The hardware clock is battery operated, and runs continuously, even if the router is powered off or rebooted.

If the software clock and hardware clock are not synchronized, and the software clock is more accurate, use this command to update the hardware clock to the correct date and time.

**Examples** The following example copies the current date and time from the software clock to the hardware clock:

```
Router> clock update-calendar
```

| Related Commands | Command                    | Description                                                                          |
|------------------|----------------------------|--------------------------------------------------------------------------------------|
|                  | <b>clock read-calendar</b> | Performs a one-time update of the software clock from the hardware clock (calendar). |
|                  | <b>ntp update-calendar</b> | Periodically updates the hardware clock from the software clock.                     |

# controller

To configure a T1, E1, or BITS controller and enter controller configuration mode, use the **controller** command in global configuration mode.

**controller** { **bits** | **t1** | **e1** | **shdsl** } *slot / port / subslot number / port number*

## Syntax Description

|                       |                                                                                                                                                                       |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bits</b>           | BITS controller                                                                                                                                                       |
| <b>t1</b>             | T1 controller.                                                                                                                                                        |
| <b>e1</b>             | E1 controller.                                                                                                                                                        |
| <b>shdsl</b>          | SHDSL controller.                                                                                                                                                     |
| <i>slot/port</i>      | Specifies the backplane slot number and port number. Refer to your hardware installation manual for the specific values and slot numbers.                             |
| <i>subslot number</i> | Specifies the subslot on the router in which the HWIC is installed.                                                                                                   |
| <i>port</i>           | Specifies the port number of the controller. Valid numbers are 0 and 1. The slash mark (/) is required between the <i>slot</i> argument and the <i>port</i> argument. |

## Command Default

No T1 or E1 controller is configured.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                                                                         |
|-------------|----------------------------------------------------------------------------------------------------------------------|
| 10.0        | This command was introduced.                                                                                         |
| 10.3        | The <b>e1</b> keyword was added.                                                                                     |
| 12.0(3)T    | Support was added for dial shelves on Cisco AS5800 access servers.                                                   |
| 12.2(7)XO   | The <b>j1</b> keyword was added for the Cisco 2600 and Cisco 3600 series.                                            |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                      |
| 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2.                                                      |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not provide support for DSL HWICs. |

## Related Commands

| Command                    | Description                                                               |
|----------------------------|---------------------------------------------------------------------------|
| <b>controllers shdsl</b>   | Enters configuration mode for the SHDSL controller.                       |
| <b>show controllers e1</b> | Displays information about the E1 controller.                             |
| <b>show controllers t1</b> | Displays the total number of calls and call durations on a T1 controller. |

# cns config initial

To enable the Cisco Networking Services (CNS) configuration agent and initiate a download of the initial configuration, use the **cns config initial** command in global configuration mode. To remove an existing **cns config initial** command from the running configuration of the routing device, use the **no** form of this command.

**cns config initial** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**page** *page*] [**syntax-check**] [**no-persist**] [**source** *interface name*] [**status** *url*] [**event**] [**inventory**]

**no cns config initial**

| Syntax Description       |                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>host-name</i>         | Hostname of the configuration server.                                                                                                                                                                                                                                                                                                                                                        |
| <i>ip-address</i>        | IP address of the configuration server.                                                                                                                                                                                                                                                                                                                                                      |
| <b>encrypt</b>           | (Optional) Uses a Secure Sockets Layer (SSL) encrypted link to the event gateway.                                                                                                                                                                                                                                                                                                            |
| <i>port-number</i>       | (Optional) Port number of the configuration service. The value is from 0 to 65535. The default is 80 with no encryption and 443 with encryption.                                                                                                                                                                                                                                             |
| <b>page</b>              | (Optional) Indicates that the configuration is located on a web page.                                                                                                                                                                                                                                                                                                                        |
| <i>page</i>              | (Optional) Web page where the configuration is located. The default is /cns/config.asp.                                                                                                                                                                                                                                                                                                      |
| <b>syntax-check</b>      | (Optional) Turns on syntax checking.                                                                                                                                                                                                                                                                                                                                                         |
| <b>no-persist</b>        | (Optional) Suppresses the default automatic writing to NVRAM of the configuration pulled as a result of issuing the <b>cns config initial</b> command. If not present, issuing the <b>cns config initial</b> command causes the resultant configuration to be automatically written to NVRAM.                                                                                                |
| <b>source</b>            | (Optional) Specifies the source of CNS communications.                                                                                                                                                                                                                                                                                                                                       |
| <i>interface name</i>    | (Optional) Interface name of the source of CNS communications.                                                                                                                                                                                                                                                                                                                               |
| <b>status</b> <i>url</i> | (Optional) Sends an event to the specified URL via HTTP, either notifying successful completion of the configuration or warning that the configuration contained errors.                                                                                                                                                                                                                     |
| <b>event</b>             | (Optional) Sends an event to the Event Bus notifying successful completion of the configuration or warning that the configuration contained errors. If the CNS event agent is not configured, the event is saved until the CNS event agent is enabled. If the <b>event</b> keyword is not specified, a log message is sent to the console of the device after the configuration is complete. |
| <b>inventory</b>         | (Optional) Sends an inventory of the line cards and modules in the router to the CNS configuration engine as part of the HTTP request.                                                                                                                                                                                                                                                       |

**Command Default** The port number defaults to 80 with no encryption and 443 with encryption. Default web page of the initial configuration is /cns/config.asp.

**Command Modes** Global configuration (config)

**Command History**

| Release     | Modification                                                                           |
|-------------|----------------------------------------------------------------------------------------|
| 12.2(2)T    | This command was introduced.                                                           |
| 12.0(18)ST  | This command was integrated into Cisco IOS Release 12.0(18)ST.                         |
| 12.0(22)S   | This command was integrated into Cisco IOS Release 12.0(22)S.                          |
| 12.2(2)XB   | This command was implemented on Cisco IAD2420 series Integrated Access Devices (IADs). |
| 12.2(8)T    | The <b>source</b> and <b>encrypt</b> keywords were added.                              |
| 12.3(1)     | The <b>inventory</b> keyword was added.                                                |
| 12.3(8)T    | The <b>status url</b> keyword/argument pair was added.                                 |
| 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.                          |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                        |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.                         |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI.                        |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                         |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                        |

**Usage Guidelines**

Use this command when a basic configuration—called a bootstrap configuration—is added to multiple routers before being deployed. When a router is initially powered (or each time a router is reloaded when the **no-persist** keyword is used) the **cns config initial** command causes a configuration file—called an initial configuration—for the router to be downloaded from the configuration server. The initial configuration can be unique for each router.

When the configuration has been received by the router, each line of the configuration is applied in the same order as it was received. If the Cisco IOS parser has an error with one of the lines of the configuration, then all the configuration up to this point is applied to the router, but none of the configuration beyond the error is applied. If an error occurs, the command retries until it successfully completes. Once the configuration has successfully completed the **cns config initial** command is removed from the running configuration. By default, NVRAM is updated except when the **no-persist** keyword is configured.

When this command is used with the **event** keyword, a single message is published on the event bus after the configuration is complete. The event bus displays one of the following status messages:

- `cisco.mgmt.cns.config.complete`—CNS configuration agent successfully applied the initial configuration.
- `cisco.mgmt.cns.config.warning`—CNS configuration agent fully applied the initial configuration but encountered possible semantic errors.

When this command is used with the **status** keyword, a single message is published to the URL specified after the configuration is complete.

**Examples**

The following example shows how to enable the CNS configuration agent and initiate an initial configuration:

```
Router(config)# cns config initial 10.19.4.5
```

**Related Commands**

| Command                        | Description                                                                                             |
|--------------------------------|---------------------------------------------------------------------------------------------------------|
| <b>cns config connect-intf</b> | Specifies the interface for connecting to the CNS configuration engine.                                 |
| <b>cns config notify</b>       | Detects CNS configuration changes and sends an event containing the previous and current configuration. |
| <b>cns config retrieve</b>     | Enables the CNS configuration agent and initiates a download of the initial configuration.              |
| <b>cns event</b>               | Configures the CNS event gateway, which provides CNS event services to Cisco IOS clients.               |
| <b>show cns config status</b>  | Displays information about the status of the CNS configuration agent.                                   |

# cns config partial

To start the Cisco Networking Services (CNS) configuration agent and accept a partial configuration, use the **cns config partial** command in global configuration mode. To shut down the CNS partial configuration agent, use the **no** form of this command.

**cns config partial** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**source** *interface name*] [**inventory**]

**no cns config partial**

## Syntax Description

|                       |                                                                                                                                                  |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>host-name</i>      | Hostname of the configuration server.                                                                                                            |
| <i>ip-address</i>     | IP address of the configuration server.                                                                                                          |
| <b>encrypt</b>        | (Optional) Uses an SSL-encrypted link between the router and the web server.                                                                     |
| <i>port-number</i>    | (Optional) Port number of the configuration service. The value is from 0 to 65535. The default is 80 with no encryption and 443 with encryption. |
| <b>source</b>         | (Optional) Specifies the source of this device.                                                                                                  |
| <i>interface name</i> | (Optional) Interface name to use as the source of this device.                                                                                   |
| <b>inventory</b>      | (Optional) Sends an inventory of the line cards and modules in the router to the CNS configuration engine as part of the HTTP request.           |

## Command Default

The CNS configuration agent is not enabled to accept a partial configuration and the router does not request or receive updates.

## Command Modes

Global configuration (config)

## Command History

| Release     | Modification                                                                           |
|-------------|----------------------------------------------------------------------------------------|
| 12.2(2)T    | This command was introduced.                                                           |
| 12.0(18)ST  | This command was integrated into Cisco IOS Release 12.0(18)ST.                         |
| 12.0(22)S   | This command was integrated into Cisco IOS Release 12.0(22)S.                          |
| 12.2(2)XB   | This command was implemented on Cisco IAD2420 series Integrated Access Devices (IADs). |
| 12.2(8)T    | The <b>source</b> keyword and <b>encrypt</b> arguments were added.                     |
| 12.3(1)     | The <b>inventory</b> keyword was added.                                                |
| 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.                          |
| 12.4(4)T    | This command was modified to include enhanced CNS error messages.                      |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                        |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.                         |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI.                        |

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

### Usage Guidelines

Use this command to start the CNS partial configuration agent. You must enable the CNS event agent using the **cns event** command before configuring this command. The CNS event agent sends an event with the subject “cisco.mgmt.cns.config.load” to specify whether configuration data can be pushed to the CNS partial configuration agent or pulled from a configuration server by the CNS partial configuration agent.

In the push model, the event message delivers the configuration data to the partial configuration agent.

In the pull model, the event message triggers the partial configuration agent to pull the configuration data from the CNS configuration engine. The event message contains information about the CNS configuration engine, not the actual configuration data. The host name or IP address is the address of the CNS configuration engine from which the configuration is pulled. Use the **cns trusted-server** command to specify which CNS configuration engines can be used by the CNS partial configuration agent.

When the configuration has been received by the router, each line of the configuration is applied in the same order as it was received. If the Cisco IOS parser has an error with one of the lines of the configuration, then all the configuration up to this point is applied to the router, but none of the configuration beyond the error is applied. If an error occurs, the command retries until the configuration successfully completes. In the pull mode, the command does not retry after an error. By default, NVRAM is updated except when the **no-persist** keyword is configured.

A message is published on the CNS event bus after the partial configuration is complete. The CNS event bus displays one of the following status messages:

- **cisco.mgmt.cns.config.complete**—CNS configuration agent successfully applied the partial configuration.
- **cisco.mgmt.cns.config.warning**—CNS configuration agent fully applied the partial configuration, but encountered possible semantic errors.
- **cisco.mgmt.cns.config.failure(CLI syntax)**—CNS configuration agent encountered a command line interface (CLI) syntax error and was not able to apply the partial configuration.
- **cisco.mgmt.cns.config.failure(CLI semantic)**—CNS configuration agent encountered a CLI semantic error and was not able to apply the partial configuration.

### Examples

The following example shows how to configure the CNS partial configuration agent to accept events from the event gateway at 172.28.129.22. The CNS partial configuration agent connects to the CNS configuration server at 172.28.129.22, port number 80. The CNS partial configuration agent requests are redirected to a configuration server at 172.28.129.40, port number 80.

```
Router(config)# cns event 172.28.129.22
Router(config)# cns trusted-server config 172.28.129.40
Router(config)# cns config partial 172.28.129.22
```

The following example shows an enhanced error message sent to the subject “cisco.mgmt.cns.config.results”:

```
[2005-09-08 14:30:44]: subject=cisco.mgmt.cns.config.results.dvlpr-7200-6, message=
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://www.w3.org/2003/05/soap-envelope">
<SOAP:Header>
```

```

<wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
SOAP:mustUnderstand="true">
<wsse:UsernameToken>
<wsse:Username>user1</wsse:Username>
<wsse:Password>password1</wsse:Password>
</wsse:UsernameToken>
</wsse:Security>
<CNS:cnsHeader Version="2.0" xmlns:CNS="http://www.cisco.com/management/cns/envelope">
<CNS:Agent>CNS_CONFIG</CNS:Agent>
<CNS:Response>
<CNS:correlationID>SOAP_IDENTIFIER</CNS:correlationID>
</CNS:Response>
<CNS:Time>2005-09-13T08:34:36.523Z</CNS:Time>
</CNS:cnsHeader>
</SOAP:Header>
<SOAP:Body xmlns="http://www.cisco.com/management/cns/config">
<configResults version="2.0" overall="Success">
<configId>AAA</configId>
</configResults>
</SOAP:Body>
</SOAP:Envelope>

```

**Related Commands**

| Command                            | Description                                                                                            |
|------------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>cns config initial</b>          | Starts the CNS configuration agent and initiates an initial configuration.                             |
| <b>cns event</b>                   | Enables and configures CNS event agent services.                                                       |
| <b>cns trusted-server</b>          | Specifies a trusted server for CNS agents.                                                             |
| <b>show cns config outstanding</b> | Displays information about incremental CNS configurations that have started but are not yet completed. |



# cns config retrieve

To enable the Cisco Networking Services (CNS) configuration agent and initiate a download of the initial configuration, use the **cns config retrieve** command in privileged EXEC mode.

**cns config retrieve** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**page** *page*]  
 [**overwrite-startup**] [**retry** *retries* **interval** *seconds*] [**syntax-check**] [**no-persist**] [**source**  
*interface name*] [**status** *url*] [**event**] [**inventory**]

| Syntax Description             |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>host-name</i>               | Hostname of the configuration server.                                                                                                                                                                                                                                                                                                                                                                                                             |
| <i>ip-address</i>              | IP address of the configuration server.                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>encrypt</b>                 | (Optional) Uses an SSL-encrypted link to the event gateway.                                                                                                                                                                                                                                                                                                                                                                                       |
| <i>port-number</i>             | (Optional) Port number of the configuration service. The value is from 0 to 65535. The default is 80 with no encryption and 443 with encryption.                                                                                                                                                                                                                                                                                                  |
| <b>page</b>                    | (Optional) Indicates that the configuration is located on a web page.                                                                                                                                                                                                                                                                                                                                                                             |
| <i>page</i>                    | (Optional) Web page where the configuration is located. The default is /cns/config.asp.                                                                                                                                                                                                                                                                                                                                                           |
| <b>overwrite-startup</b>       | (Optional) Replaces the startup configuration file. Does not apply to the running configuration file.                                                                                                                                                                                                                                                                                                                                             |
| <b>retry</b> <i>retries</i>    | (Optional) Specifies the retry interval. The range is 0 to 100. The default is 0.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>interval</b> <i>seconds</i> | (Optional) Specifies the time in seconds, before the next attempt to request the configuration of a device from a configuration server. The range is 1 to 3600.                                                                                                                                                                                                                                                                                   |
| <b>syntax-check</b>            | (Optional) Turns on syntax checking.                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>no-persist</b>              | (Optional) Suppresses the default automatic writing to NVRAM of the configuration pulled as a result of issuing the <b>cns config retrieve</b> command. If not present, issuing the <b>cns config retrieve</b> command causes the resultant configuration to be automatically written to NVRAM.                                                                                                                                                   |
| <b>source</b>                  | (Optional) Specifies the source of CNS communications.                                                                                                                                                                                                                                                                                                                                                                                            |
| <i>interface name</i>          | (Optional) Interface name of the source of the configuration.                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>status</b> <i>url</i>       | (Optional) Sends the configuration the specified URL via HTTP, either notifying successful completion of the configuration or warning that the configuration contained errors.                                                                                                                                                                                                                                                                    |
| <b>event</b>                   | (Optional) Sends an event to the CNS Event Bus stating successful completion of the configuration, a warning that the configuration contained errors, or a message noting that the configuration failed. If the CNS event agent is not configured, the event is saved until the CNS event agent is enabled. If the <b>event</b> keyword is not specified, a log message is sent to the console of the device after the configuration is complete. |
| <b>inventory</b>               | (Optional) Sends an inventory of the line cards and modules in the router to the CNS configuration engine as part of the HTTP request.                                                                                                                                                                                                                                                                                                            |

## Command Default

The port number defaults to 80 with no encryption and 443 with encryption.  
 Default web page of the initial configuration is /cns/config.asp.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification                                                                                          |
|-----------------|-------------|-------------------------------------------------------------------------------------------------------|
|                 | 12.2(2)T    | This command was introduced.                                                                          |
|                 | 12.0(18)ST  | This command was integrated into Cisco IOS Release 12.0(18)ST.                                        |
|                 | 12.0(22)S   | This command was integrated into Cisco IOS Release 12.0(22)S.                                         |
|                 | 12.3(1)     | The <b>inventory</b> keyword was added.                                                               |
|                 | 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.                                         |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                       |
|                 | 12.4(15)T   | The <b>retry</b> <i>retries</i> and <b>interval</b> <i>seconds</i> keywords and arguments were added. |
|                 | 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC.                                       |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.                                        |
|                 | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI.                                       |
|                 | 12.4(20)MR  | This command was incorporated.                                                                        |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                       |

### Usage Guidelines

Use this command to request the configuration of a device from a configuration server. Use the **cns trusted-server** command to specify which configuration server can be used (trusted).

When the configuration has been received by the router, each line of the configuration is applied in the same order as it was received. If the Cisco IOS parser has an error with one of the lines of the configuration, then all the configuration up to this point is applied to the router, but none of the configuration beyond the error is applied. If an error occurs, the command does not retry.

A single message is published on the event bus after the partial configuration is complete. The event bus displays one of the following status messages:

- cisco.mgmt.cns.config.complete—CNS configuration agent successfully applied the configuration.
- cisco.mgmt.cns.config.warning—CNS configuration agent fully applied the configuration, but encountered possible semantic errors.
- cisco.mgmt.cns.config.failure—CNS configuration agent encountered an error and was not able to apply the configuration.

The **cns config retrieve** command can be used with Command Scheduler commands (for example, **kron policy-list** and **cli** commands) in environments where it is not practical to use the CNS event agent and the **cns config partial** command. Configured within the **cli** command, the **cns config retrieve** command can be used to poll the configuration server to detect configuration changes.

You can use the optional **retry** and **interval** keywords to specify an amount of time in seconds to wait before attempting to retrieve a configuration from a trusted server. The number of retries is restricted to 100 to prevent the configuration agent from indefinitely attempting to reach an unreachable server. Use the keyboard combination **Ctrl-Shift-6** to abort this command.

### Examples

The following example shows how to request a configuration from a trusted server at 10.1.1.1:

```
Router(config)# cns trusted-server all 10.1.1.1
Router(config)# exit
```

```
Router# cns config retrieve 10.1.1.1
```

The following example shows how to request a configuration from a trusted server at 10.1.1.1 and to configure a CNS configuration retrieve interval:

```
Router(config)# cns trusted-server all 10.1.1.1
Router(config)# exit
Router# cns config retrieve 10.1.1.1 retry 50 interval 1500
CNS Config Retrieve Attempt 1 out of 50 is in progress
Next cns config retrieve retry is in 1499 seconds (Ctrl-Shift-6 to abort this command).
..
00:26:40: %CNS-3-TRANSPORT: CNS_HTTP_CONNECTION_FAILED:10.1.1.1 -Process= "CNS config
retv", ipl= 0, pid= 43
00:26:40: %CNS-3-TRANSPORT: CNS_HTTP_CONNECTION_FAILED -Process= "CNS config retv", ipl=
0, pid= 43.....
```

## Related Commands

| Command                       | Description                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------|
| <b>cli</b>                    | Specifies EXEC CLI commands within a Command Scheduler policy list.                        |
| <b>cns config initial</b>     | Starts the CNS configuration agent and initiates an initial configuration.                 |
| <b>cns trusted-server</b>     | Specifies a trusted server for CNS agents.                                                 |
| <b>kron policy-list</b>       | Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode. |
| <b>show cns config status</b> | Displays information about the status of the CNS configuration agent.                      |

## cns event

To configure the Cisco Networking Services (CNS) event gateway, which provides CNS event services to Cisco IOS clients, use the **cns event** command in global configuration mode. To remove the specified event gateway from the gateway list, use the **no** form of this command.

```
cns event {host-name | ip-address} [encrypt] [port-number] [backup] [failover-time seconds]
[keepalive seconds retry-count] [source interface-name] [clock-timeout time] [reconnect
time]
```

```
no cns event [host-name | ip-address] [port-number] [encrypt] [backup] [failover-time seconds]
[keepalive seconds retry-count] [source interface name] [clock-timeout time] [reconnect
time]
```

### Syntax Description

|                                                    |                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>host-name</i>                                   | Hostname of the event gateway.                                                                                                                                                                                                                                                                |
| <i>ip-address</i>                                  | IP address of the event gateway.                                                                                                                                                                                                                                                              |
| <b>encrypt</b>                                     | (Optional) Uses an SSL-encrypted link to the event gateway.<br><br><b>Note</b> This keyword is available only in images that support SSL.                                                                                                                                                     |
| <i>port-number</i>                                 | (Optional) Port number for the event gateway.<br><br><ul style="list-style-type: none"> <li>Valid range is from 0 to 65535. The default is 11011 with no encryption or 11012 with encryption.</li> </ul>                                                                                      |
| <b>backup</b>                                      | (Optional) Indicates a backup gateway.<br><br><ul style="list-style-type: none"> <li>If omitted, indicates the primary gateway. A primary gateway must be configured before you can configure a backup gateway. Optional keywords, if omitted, are set as for the primary gateway.</li> </ul> |
| <b>failover-time</b> <i>seconds</i>                | (Optional) Specifies a time interval, in seconds, to wait for the primary gateway route after the route to the backup gateway is established.<br><br><ul style="list-style-type: none"> <li>Valid range is from 0 to 65535. The default is 3.</li> </ul>                                      |
| <b>keepalive</b> <i>seconds</i> <i>retry-count</i> | (Optional) Specifies a keepalive timeout, in seconds, and retry count.                                                                                                                                                                                                                        |
| <b>source</b> <i>interface-name</i>                | (Optional) Indicates the interface name of the source for CNS communications.                                                                                                                                                                                                                 |
| <b>clock-timeout</b> <i>time</i>                   | (Optional) Specifies the maximum time, in minutes, that the CNS event agent waits for the clock to be set for transports (such as SSL) that require an accurate clock. The default is 10.                                                                                                     |
| <b>reconnect</b> <i>time</i>                       | (Optional) Specifies the configurable upper limit of the maximum retry timeout, in seconds.<br><br><ul style="list-style-type: none"> <li>The valid range is from 1 to 65535. The default is 3600.</li> </ul>                                                                                 |

### Command Default

No CNS event gateway is configured.

**Command Modes** Global configuration (config)

| Command History | Release     | Modification                                                                                                                                                             |
|-----------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.2(2)T    | This command was introduced.                                                                                                                                             |
|                 | 12.0(18)ST  | This command was integrated into the Cisco IOS Release 12.0(18)ST.                                                                                                       |
|                 | 12.0(22)S   | This command was integrated into Cisco IOS Release 12.0(22)S.                                                                                                            |
|                 | 12.2(2)XB   | This command was implemented on Cisco IAD2420 series Integrated Access Devices (IADs).                                                                                   |
|                 | 12.2(8)T    | The <b>encrypt</b> , <b>init-retry</b> , <b>source</b> , and <b>force-fmt1</b> keywords were added.                                                                      |
|                 | 12.3        | The <b>reconnect-time</b> keyword was added.                                                                                                                             |
|                 | 12.3(1)     | The <b>init-retry</b> keyword was replaced with the <b>failover-time</b> keyword. The <b>force-fmt1</b> keyword was removed. The <b>clock-timeout</b> keyword was added. |
|                 | 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.                                                                                                            |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                          |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.                                                                                                           |
|                 | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI.                                                                                                          |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                           |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                          |

**Usage Guidelines**

The CNS event agent must be enabled before any of the other CNS agents are configured because the CNS event agent provides a transport connection to the CNS event bus for all other CNS agents. The other CNS agents use the connection to the CNS event bus to send and receive messages. The CNS event agent does not read or modify the messages.

The **failover-time** keyword is useful if you have a backup CNS event gateway configured. If the CNS event agent is trying to connect to the gateway and it discovers that the route to the backup is available before the route to the primary gateway, the *seconds* argument specifies how long the CNS event agent continues to search for a route to the primary gateway before attempting to link to the backup gateway.

Unless you are using a bandwidth-constrained link, you should set a keepalive timeout and retry count. Doing so allows the management network to recover gracefully should a Cisco IE2100 configuration engine ever fail. Without the keepalive data, such a failure requires manual intervention on every device. The value of the *seconds* argument multiplied by the value of the *retry-count* argument determines the length of idle time before the CNS event agent disconnects and attempts to reconnect to the gateway. We recommend a minimum *retry-count* of two.

If the optional **source** keyword is used, the source IP address might be a secondary IP address of a specific interface to allow a management network to run on top of a production network.

If network connectivity between the Cisco IOS router running the CNS event agent and the gateway is absent, the event agent goes into an exponential backoff retry mode and gets stuck at the maximum limit (which may be hours). The **reconnect-time** keyword allows a configurable upper limit of the maximum retry timeout.

If you configure CNS passwords using the **cns password** command, existing event connections are closed and reopened.

### Examples

The following example shows how to set the address of the primary CNS event gateway to the configuration engine software running on IP address 10.1.2.3, port 11011, with a keepalive of 60 seconds and a retry count of 5:

```
Router(config)# cns event 10.1.2.3 11011 keepalive 60 5
```

### Related Commands

| Command                      | Description                                                            |
|------------------------------|------------------------------------------------------------------------|
| <b>cns id</b>                | Sets the unique event ID, config ID, or image ID used by CNS services. |
| <b>cns password</b>          | Configures a CNS password.                                             |
| <b>show cns event status</b> | Displays status information about the CNS event agent.                 |

## cns exec

To enable and configure the Cisco Networking Services (CNS) exec agent, which provides CNS exec agent services to Cisco IOS clients, use the **cns exec** command in global configuration mode. To disable the use of CNS exec agent services, use the **no** form of this command.

**cns exec** [*host-name* | *ip-address*] [**encrypt** [*enc-port-number*]] [*port-number*]  
[**source** *interface name*]

**no cns exec** [*host-name* | *ip-address*] [**encrypt** [*enc-port-number*]] [*port-number*]  
[**source** *interface name*]

### Syntax Description

|                        |                                                                                                                                           |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <i>host-name</i>       | (Optional) Hostname of the exec server.                                                                                                   |
| <i>ip-address</i>      | (Optional) IP address of the exec server.                                                                                                 |
| <b>encrypt</b>         | (Optional) Uses an SSL-encrypted link to the exec agent server.<br><b>Note</b> This keyword is available only in images that support SSL. |
| <i>enc-port-number</i> | (Optional) Port number for the encrypted exec server. The default is 443.                                                                 |
| <i>port-number</i>     | (Optional) Port number for the exec server. The default is 80.                                                                            |
| <b>source</b>          | (Optional) Specifies the use of an IP address defined by the <i>ip-address</i> argument as the source for CNS exec agent communications.  |
| <i>interface name</i>  | (Optional) Interface name.                                                                                                                |

### Command Default

No CNS exec agent is configured.

### Command Modes

Global configuration (config)

### Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.3(1)     | This command was introduced.                                    |
| 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.   |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

### Usage Guidelines

The CNS exec agent allows a remote application to execute an EXEC mode command-line interface (CLI) command on a Cisco IOS device by sending an event message containing the command. A restricted set of EXEC CLI commands are supported, including **show** commands.

In previous Cisco IOS releases, the CNS exec agent was enabled when the CNS configuration agent was enabled through the **cns config partial** command.

---

**Examples**

The following example shows how to enable the CNS exec agent with an IP address of 10.1.2.3 for the exec agent server, a port number of 93, and a source IP address of 172.17.2.2:

```
Router(config)# cns exec 10.1.2.3 93 source 172.17.2.2
```

---

**Related Commands**

| Command                       | Description                                                                         |
|-------------------------------|-------------------------------------------------------------------------------------|
| <b>cns event</b>              | Enables and configures CNS event agent services.                                    |
| <b>show cns event subject</b> | Displays a list of CNS event agent subjects that are subscribed to by applications. |



# cns id

To set the unique event ID, config ID, or image ID used by Cisco Networking Services (CNS), use the **cns id** command in global configuration mode. To set the identifier to the hostname of the Cisco IOS device, use the **no** form of this command.

## If ID Choice Is an IP Address or MAC Address

```
cns id type number {ipaddress | mac-address} [event | image]
```

```
no cns id type number {ipaddress | mac-address} [event | image]
```

## If ID Choice Is Anything Else

```
cns id {hardware-serial | hostname | string string | udi} [event | image]
```

```
no cns id {hardware-serial | hostname | string string | udi} [event | image]
```

| Syntax Description          |                                                                                                                                                 |                                                                                                                                                              |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>type number</i>          | Type of interface (for example, <b>ethernet</b> , <b>group-async</b> , <b>loopback</b> , or <b>virtual-template</b> ) and the interface number. | <ul style="list-style-type: none"> <li>Indicates from which interface the IP or MAC address should be retrieved in order to define the unique ID.</li> </ul> |
| <b>ipaddress</b>            | Uses the IP address specified in the <i>type number</i> arguments as the unique ID.                                                             |                                                                                                                                                              |
| <b>mac-address</b>          | Uses the MAC address specified in the <i>type number</i> arguments as the unique ID.                                                            |                                                                                                                                                              |
| <b>event</b>                | (Optional) Sets this ID to be the event ID value, which is used to identify the Cisco IOS device for CNS event services.                        | <ul style="list-style-type: none"> <li>If both optional keywords are omitted, the event ID is set to the hostname of the Cisco IOS device.</li> </ul>        |
| <b>image</b>                | (Optional) Sets this ID to be the image ID value, which is used to identify the Cisco IOS device for CNS image agent services.                  | <ul style="list-style-type: none"> <li>If both optional keywords are omitted, the image ID is set to the hostname of the Cisco IOS device.</li> </ul>        |
| <b>hardware-serial</b>      | Uses the hardware serial number as the unique ID.                                                                                               |                                                                                                                                                              |
| <b>hostname</b>             | Uses the hostname as the unique ID. This is the system default.                                                                                 |                                                                                                                                                              |
| <b>string</b> <i>string</i> | Uses an arbitrary text string—typically the hostname—as the unique ID.                                                                          |                                                                                                                                                              |
| <b>udi</b>                  | Uses the product Unique Device Identifier as the unique ID.                                                                                     |                                                                                                                                                              |

**Command Default** The system defaults to the hostname of the Cisco IOS device as the unique ID.

**Command Modes** Global configuration (config)

**Command History**

| Release     | Modification                                                                                             |
|-------------|----------------------------------------------------------------------------------------------------------|
| 12.2(2)XB   | This command was introduced on Cisco IAD2420 series IADs.                                                |
| 12.2(8)T    | This command was integrated into Cisco IOS Release 12.2(8)T. The <b>dns-reverse</b> keyword was removed. |
| 12.3(1)     | The optional <b>image</b> keyword was added to set an image ID.                                          |
| 12.3(14)T   | The <b>udi</b> keyword was added to use the product UDI as the unique ID.                                |
| 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.                                            |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                          |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.                                           |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI.                                          |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                           |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                          |

**Usage Guidelines**

Use this command to set the unique ID to the CNS configuration agent, which then pulls the initial configuration template to the Cisco IOS device during bootup.

You can set one or all three IDs: the config ID value for CNS configuration services, the event ID value for CNS event services, and the image ID value for CNS image agent services. To set all values, use the command three times.

To set the CNS event ID to the host name of the Cisco IOS device, use the **no** form of this command with the **event** keyword. To set the CNS config ID to the host name of the Cisco IOS device, use the **no** form of this command without the **event** keyword. To set the CNS image ID to the host name of the Cisco IOS device, use the **no** form of this command with the **image** keyword.

**Unique Device Identifier**

Each identifiable Cisco product is an entity, as defined by the Entity MIB (RFC-2737) and its supporting documents. Some entities, such as a chassis, have subentities like slots. An Ethernet switch might be a member of a superentity, such as a stack. Most Cisco entities that are orderable products leave the factory with an assigned UDI. The UDI information is printed on a label that is affixed to the physical hardware device, and it is also stored electronically on the device in order to facilitate remote retrieval. To use UDI retrieval, the Cisco product in use must be UDI-enabled.

A UDI consists of the following elements:

- Product identifier (PID)
- Version identifier (VID)
- Serial number (SN)

The PID is the name by which a product can be ordered; historically, it has been called the “Product Name” or “Part Number.” This identifier is the one to use to order an exact replacement part.

The VID is the version of the product. When a product is revised, the VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product carries a unique serial number assigned at the factory, which cannot be changed in the field. The serial number is used to identify an individual, specific instance of a product.

**Note**

The **udi** keyword creates an ID consisting of the PID, VID, and SN values. Any spaces in PID, VID and SN values are removed. To view the UDI for this product, use the **show inventory** command. This keyword is not available in Cisco IOS Release 12.2(33)SRA.

**Examples**

The following example shows how to pass the hostname of the Cisco IOS device as the config ID value:

```
Router(config)# cns id hostname
```

The following example shows how to pass the hardware serial number of the Cisco IOS device as the event ID value:

```
Router(config)# cns id hardware-serial event
```

The following example shows how to pass the UDI as the event ID value:

```
Router(config)# cns id udi event
```

The following example shows how to pass the IP address of Ethernet interface 0/1 as the image ID value:

```
Router(config)# cns id ethernet 0/1 image
```

**Related Commands**

| Command               | Description                                                                                              |
|-----------------------|----------------------------------------------------------------------------------------------------------|
| <b>cns event</b>      | Enables the CNS event gateway, which provides CNS event services to Cisco IOS clients.                   |
| <b>cns image</b>      | Enables the CNS image agent services to Cisco IOS clients.                                               |
| <b>show inventory</b> | Displays the product inventory listing for all Cisco products that are installed in a networking device. |

# cns image password

To configure a password to use with the Cisco Networking Services (CNS) image agent services, use the **cns image password** command in global configuration mode. To disable the use of a password, use the **no** form of this command.

**cns image password** *image-password*

**no cns image password** *image-password*

## Syntax Description

|                       |                                                   |
|-----------------------|---------------------------------------------------|
| <i>image-password</i> | Password to be used for CNS image agent services. |
|-----------------------|---------------------------------------------------|

## Command Default

No password is used with the CNS image agent services.

## Command Modes

Global configuration (config)

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.3(1)     | This command was introduced.                                    |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

Use this command to create a password that is sent with the image ID in all CNS image agent messages. The recipient of these messages can use this information to authenticate the sending device. This password may be different from the username and password used for HTTP basic authentication configured with other CNS image agent commands.

## Examples

The following example shows how to configure a password to be used for the CNS image agent services:

```
Router(config)# cns image password textabc
```

## Related Commands

| Command       | Description                                                            |
|---------------|------------------------------------------------------------------------|
| <b>cns id</b> | Sets the unique event ID, config ID, or image ID used by CNS services. |

# cns image retrieve

To contact a Cisco Networking Services (CNS) image distribution server and download a new image if a new image exists, use the **cns image retrieve** command in privileged EXEC mode.

**cns image retrieve** [**server** *server-url* [**status** *status-url*]]

## Syntax Description

|                   |                                                                                                                                          |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>server</b>     | (Optional) Specifies an image distribution server to contact for information about an updated image to be downloaded.                    |
| <i>server-url</i> | (Optional) URL used to contact an image distribution server.                                                                             |
| <b>status</b>     | (Optional) Specifies that any status messages generated by this command are sent to the URL specified by the <i>status-url</i> argument. |
| <i>status-url</i> | (Optional) URL of a web server to which status messages are written.                                                                     |

## Command Default

An error occurs when a CNS image server has not previously been configured in global configuration mode.

## Usage Guidelines

When the **cns image retrieve** command is issued in privileged EXEC mode without the **server** keyword and *server-url* argument, an error occurs.

When a **cns image** server has been configured and the **cns image retrieve** command is issued with no **server** keyword and *server-url* argument, the server path configured in the **cns image** command is used.

When the **cns image** command is issued in global configuration mode with the optional **server** keyword, no keywords are required and no error occurs when you issue the **cns image retrieve** command in privileged EXEC mode.

## Command Modes

Privileged EXEC (#)

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.3(1)     | This command was introduced.                                    |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

You must enable the CNS image agent services using the **cns image** command before configuring this command.

Use this command to poll an image distribution server and download a new image to the Cisco IOS device if a new image exists.

---

**Examples**

The following example shows how to configure the CNS image agent to access the image distribution server at 10.19.2.3 and download a new image if a new image exists:

```
Router# cns image retrieve server https://10.20.2.3:8080/cns/imageserver/ status  
https://10.20.2.3:8080/cns/imageserver/messages/
```

---

**Related Commands**

| Command                      | Description                                            |
|------------------------------|--------------------------------------------------------|
| <b>cns image</b>             | Enables CNS image agent services.                      |
| <b>cns trusted-server</b>    | Specifies a trusted server for CNS agents.             |
| <b>show cns image status</b> | Displays information about the CNS image agent status. |

# cns inventory

To enable the CNS inventory agent—that is, to send an inventory of the router’s line cards and modules to the CNS configuration engine—and enter CNS inventory mode, use the **cns inventory** command in global configuration mode. To disable the CNS inventory agent, use the **no** form of this command.

**cns inventory**

**no cns inventory**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The CNS inventory agent is disabled.

**Command Modes** Global configuration

| Command History | Release     | Modification                                                                    |
|-----------------|-------------|---------------------------------------------------------------------------------|
|                 | 12.2(8)T    | This command was introduced.                                                    |
|                 | 12.3(1)     | The <b>config</b> , <b>event</b> , and <b>notify oir</b> keywords were removed. |
|                 | 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.                   |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                 |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                  |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                 |

**Usage Guidelines** Use this command with the **announce config** and **transport event** CNS inventory configuration mode commands to specify when to notify the CNS configuration engine of changes to the router’s port-adaptor and interface inventory. A transport must be specified in CNS inventory configuration mode before any of the CNS inventory commands are executed.

**Examples** The following example shows how to enable the CNS inventory agent and enter CNS inventory configuration mode:

```
Router(config)# cns inventory
Router(cns_inv)#
```

| Related Commands | Command                   | Description                                                                |
|------------------|---------------------------|----------------------------------------------------------------------------|
|                  | <b>cns config initial</b> | Starts the CNS configuration agent and initiates an initial configuration. |

# cns password

To configure a Cisco Networking Services (CNS) password, use the **cns password** command in global configuration mode. To disable the CNS password, use the **no** form of this command.

**cns password** *password*

**no cns password** *password*

|                           |                                                                       |
|---------------------------|-----------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>password</i> Any character string that specifies the CNS password. |
|---------------------------|-----------------------------------------------------------------------|

|                        |                                   |
|------------------------|-----------------------------------|
| <b>Command Default</b> | A CNS password is not configured. |
|------------------------|-----------------------------------|

|                      |                               |
|----------------------|-------------------------------|
| <b>Command Modes</b> | Global configuration (config) |
|----------------------|-------------------------------|

|                        |                |                                                                 |
|------------------------|----------------|-----------------------------------------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                             |
|                        | 12.4(8)T       | This command was introduced.                                    |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                                                                                                                                                                                                                                                                                            |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | You must configure the CNS password the first time a router is deployed, and the CNS password must be the same as the bootstrap password set on the Configuration Engine (CE). If both the router and the CE bootstrap password use their default settings, a newly deployed router can connect to the CE. |
|                         | Once connected, the CE changes the CNS password from the bootstrap password to a random password. Network administrators must ensure not to change the CNS password. If the CNS password is changed, connectivity to the CE are lost.                                                                      |

|                 |                                                                        |
|-----------------|------------------------------------------------------------------------|
| <b>Examples</b> | The following example shows how to set a CNS password named password1: |
|-----------------|------------------------------------------------------------------------|

```
Router(config)# cns password password1
```

|                         |                |                                                                      |
|-------------------------|----------------|----------------------------------------------------------------------|
| <b>Related Commands</b> | <b>Command</b> | <b>Description</b>                                                   |
|                         | <b>cns id</b>  | Sets a unique event ID, config ID, or image ID used by CNS services. |



# cns template connect

To enter Cisco Networking Services (CNS) template connect configuration mode and define the name of a CNS connect template, use the **cns template connect** command in global configuration mode. To disable the CNS connect template, use the **no** form of this command.

**cns template connect** *name*

**no cns template connect** *name*

## Syntax Description

|             |                                                    |
|-------------|----------------------------------------------------|
| <i>name</i> | Name of the CNS connect template to be configured. |
|-------------|----------------------------------------------------|

## Command Default

No CNS connect templates are defined.

## Command Modes

Global configuration (config)

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.3(2)XF   | This command was introduced.                                    |
| 12.3(8)T    | This command was integrated into Cisco IOS Release 12.3(8)T.    |
| 12.3(9)     | This command was integrated into Cisco IOS Release 12.3(9).     |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

Use the **cns template connect** command to enter CNS template connect configuration mode and define the name of the CNS connect template to be configured. Then use the **cli** command to specify the command lines of the CNS connect template.



### Note

When you create a CNS connect template, you must enter the **exit** command to complete the configuration of the template and exit from CNS template connect configuration mode. This requirement was implemented to prevent accidentally entering a command without the **cli** command.

## Examples

The following example shows how to configure a CNS connect template named template1:

```
Router(config)# cns template connect template1
Router(config-templ-conn)# cli command-1
Router(config-templ-conn)# cli command-2
Router(config-templ-conn)# cli no command-3
Router(config-templ-conn)# exit
```

```
Router(config)#
```

When the `template1` template is applied, the following commands are sent to the router's parser:

```
command-1
command-2
no command-3
```

When the `template1` template is removed from the router's configuration after an unsuccessful ping attempt to the CNS configuration engine, the following commands are sent to the router's parser:

```
no command-1
no command-2
command-3
```

#### Related Commands

| Command               | Description                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>cli (cns)</b>      | Specifies the command lines of a CNS connect template.                                                                                    |
| <b>cns connect</b>    | Enters CNS connect configuration mode and defines the parameters of a CNS connect profile for connecting to the CNS configuration engine. |
| <b>discover (cns)</b> | Defines the interface parameters within a CNS connect profile for connecting to the CNS configuration engine.                             |
| <b>template (cns)</b> | Specifies a list of CNS connect templates within a CNS connect profile to be applied to a router's configuration.                         |

## cns trusted-server

To specify a trusted server for Cisco Networking Services (CNS) agents, use the **cns trusted-server** command in global configuration mode. To disable the use of a trusted server for a CNS agent, use the **no** form of this command.

**cns trusted-server** {all-agents | config | event | exec | image} *name*

**no cns trusted-server** {all-agents | config | event | exec | image} *name*

### Syntax Description

|                   |                                                                           |
|-------------------|---------------------------------------------------------------------------|
| <b>all-agents</b> | Specifies a trusted server for all CNS agents.                            |
| <b>config</b>     | Specifies a trusted server for CNS config agent.                          |
| <b>event</b>      | Specifies a trusted server for CNS event agent.                           |
| <b>exec</b>       | Specifies a trusted server for CNS exec agent.                            |
| <b>image</b>      | Specifies a trusted server for CNS image agent.                           |
| <i>name</i>       | A string that specifies the hostname or IP address of the trusted server. |

### Command Default

By default, only the implicit server strings are trusted.

The configuration of the CNS event agent's server string through the command-line interface (CLI) results in an implicit trust by all CNS agents. For the other CNS agents, the configuration of a server string using the CLI results in an implicit trust of the server for the specified agent. For example, **cns exec 10.2.1.2** implies the string 10.2.1.2 is implicitly trusted by the exec agent, and specifying **cns event 10.4.2.2** implies the string 10.4.2.2 is implicitly trusted by all the CNS agents.

### Command Modes

Global configuration (config)

### Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.3(1)     | This command was introduced.                                    |
| 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.   |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

### Usage Guidelines

Use the **cns trusted-server** command to specify a trusted server for an individual CNS agent or all the CNS agents. In previous Cisco IOS Releases, CNS agents could connect to any server and this could expose the system to security violations. An attempt to connect to a server not on the list results in an error message being displayed and an authentication failure reply extensible markup language (XML). For backwards compatibility the configuration of a server address using the configuration CLI for a CNS agent results in an implicit trust of the server for the specified agent.

Use this command when a CNS agent redirects its response to a server address that is not explicitly configured on the command line for the specific CNS agent. For example, the CNS exec agent may have one server configured but receive a message from the CNS Event Bus that overrides the configured server. The new server address string has not been explicitly configured so the new server address is not a trusted server. An error is generated when the CNS exec agent tries to respond to this new server address unless the **cns trusted-server** command has been configured for the new server address string.

The **cns trusted-server** command does not use Domain Name System (DNS). Instead a string comparison is done between the configured and implicit trusted servers and requested redirected server address.

## Examples

The following example shows how to configure server 10.19.2.5 as a trusted server for the CNS event agent:

```
Router# cns trusted-server event 10.19.2.5
```

The following example shows how to configure server 10.2.2.8, which maps though DNS to host.somedomain.com as a trusted server for all CNS agents:

```
Router# cns trusted-server all-agents 10.2.2.8
Router# cns trusted-server all-agents host
Router# cns trusted-server all-agents host.somedomain.com
```

The following example shows how to configure the string 10.2.2.8 as an implicit trusted server for the CNS image agent:

```
Router# cns image server 10.2.2.8 status 10.2.2.8
```

## Related Commands

| Command           | Description                                      |
|-------------------|--------------------------------------------------|
| <b>cns config</b> | Configures CNS configuration agent services.     |
| <b>cns event</b>  | Enables and configures CNS event agent services. |
| <b>cns image</b>  | Configures CNS image agent services.             |

# dejitter-buffer

To configure the size of the dejitter buffer, use the **dejitter-buffer** command in CEM configuration mode. To restore the dejitter buffer to its default size, use the **no** form of this command.

**dejitter-buffer** *size*

**no dejitter-buffer**

| Syntax Description | <i>size</i> | Specifies the size of the dejitter buffer, in milliseconds. The range is 4 to 500 ms; the default is 4. |
|--------------------|-------------|---------------------------------------------------------------------------------------------------------|
|--------------------|-------------|---------------------------------------------------------------------------------------------------------|

| Command Default | 4 |
|-----------------|---|
|-----------------|---|

| Command Modes | CEM configuration |
|---------------|-------------------|
|---------------|-------------------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.3(7)T    | This command was introduced.                                    |
|                 | 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Examples** The following example shows how to specify the size of the dejitter buffer:

```
Router# config t
Router(config)# interface cem 0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# dejitter-buffer 10
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

| Related Commands | Command          | Description                                                                                                             |
|------------------|------------------|-------------------------------------------------------------------------------------------------------------------------|
|                  | <b>cem</b>       | Enters circuit emulation configuration mode.                                                                            |
|                  | <b>cem class</b> | Applies the CEM interface parameters defined in the given CEM class name to the circuit.                                |
|                  | <b>class cem</b> | Configures CEM interface parameters in a class that is applied to CEM interfaces together in global configuration mode. |

# dscp

To change the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value, use the **dscp** command in random-detect-group configuration mode. To return the minimum and maximum packet thresholds to the default for the DSCP value, use the **no** form of this command.

**dscp** *dscp-value min-threshold max-threshold [mark-probability-denominator]*

**no dscp** *dscp-value min-threshold max-threshold [mark-probability-denominator]*

## Syntax Description

|                                     |                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>dscp-value</i>                   | Specifies the DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: <b>ef</b> , <b>af11</b> , <b>af12</b> , <b>af13</b> , <b>af21</b> , <b>af22</b> , <b>af23</b> , <b>af31</b> , <b>af32</b> , <b>af33</b> , <b>af41</b> , <b>af42</b> , <b>af43</b> , <b>cs1</b> , <b>cs2</b> , <b>cs3</b> , <b>cs4</b> , <b>cs5</b> , or <b>cs7</b> . |
| <i>min-threshold</i>                | Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, Weighted Random Early Detection (WRED) randomly drops some packets with the specified DSCP value.                                                                                                                              |
| <i>max-threshold</i>                | Maximum threshold in number of packets. The value range of this argument is the value of the <i>min-threshold</i> argument to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP value.                                                                                                                                  |
| <i>mark-probability-denominator</i> | (Optional) Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, one out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is from 1 to 65536. The default is 10; one out of every ten packets is dropped at the maximum threshold.       |

## Command Default

If WRED is using the DSCP value to calculate the drop probability of a packet, all entries of the DSCP table are initialized with the default settings shown in [Table 2](#) of the “Usage Guidelines” section.

## Command Modes

Random-detect-group configuration

## Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.1(5)T    | This command was introduced.                                                                                                                                                      |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

**Usage Guidelines**

This command must be used in conjunction with the **random-detect-group** command.

Additionally, the **dscp** command is available only if you specified the *dscp-based* argument when using the **random-detect-group** command.

Table 2 lists the DSCP default settings used by the **dscp** command including the DSCP value, and its corresponding minimum threshold, maximum threshold, and mark probability. The last row of the table (the row labeled “default”) shows the default settings used for any DSCP value not specifically shown in the table.

**Table 2** *dscp Default Settings*

| <b>DSCP<br/>(Precedence)</b> | <b>Minimum<br/>Threshold</b> | <b>Maximum<br/>Threshold</b> | <b>Mark<br/>Probability</b> |
|------------------------------|------------------------------|------------------------------|-----------------------------|
| af11                         | 32                           | 40                           | 1/10                        |
| af12                         | 28                           | 40                           | 1/10                        |
| af13                         | 24                           | 40                           | 1/10                        |
| af21                         | 32                           | 40                           | 1/10                        |
| af22                         | 28                           | 40                           | 1/10                        |
| af23                         | 24                           | 40                           | 1/10                        |
| af31                         | 32                           | 40                           | 1/10                        |
| af32                         | 28                           | 40                           | 1/10                        |
| af33                         | 24                           | 40                           | 1/10                        |
| af41                         | 32                           | 40                           | 1/10                        |
| af42                         | 28                           | 40                           | 1/10                        |
| af43                         | 24                           | 40                           | 1/10                        |
| cs1                          | 22                           | 40                           | 1/10                        |
| cs2                          | 24                           | 40                           | 1/10                        |
| cs3                          | 26                           | 40                           | 1/10                        |
| cs4                          | 28                           | 40                           | 1/10                        |
| cs5                          | 30                           | 40                           | 1/10                        |
| cs6                          | 32                           | 40                           | 1/10                        |
| cs7                          | 34                           | 40                           | 1/10                        |
| ef                           | 36                           | 40                           | 1/10                        |
| rsvp                         | 36                           | 40                           | 1/10                        |
| default                      | 20                           | 40                           | 1/10                        |

**Examples**

The following example enables WRED to use the DSCP value af22. The minimum threshold for the DSCP value af22 is 28, the maximum threshold is 40, and the mark probability is 10.

```
Router> enable
Router# configure terminal
Router(config)# random-detect-group class1 dscp-based
Router(cfg-red-group)# dscp af22 28 40 10
Router(cfg-red-group)# end
```

| Related Commands | Command                        | Description                                             |
|------------------|--------------------------------|---------------------------------------------------------|
|                  | <b>random-detect-group</b>     | Enables per-VC WRED or per-VC DWRED.                    |
|                  | <b>show queueing</b>           | Lists all or selected configured queueing strategies.   |
|                  | <b>show queueing interface</b> | Displays the queueing statistics of an interface or VC. |



# encapsulation (ATM)

To configure the ATM adaptation layer (AAL) and encapsulation type for an ATM virtual circuit (VC), VC class, VC, bundle, or permanent virtual circuit (PVC) range, use the **encapsulation** command in the appropriate mode. To remove an encapsulation type, use the **no** form of this command.

**encapsulation** {**aal5snap**} [**group** *group-name*]

**no encapsulation** {**aal5snap**} [**group** *group-name*]

## Syntax Description

|                   |                                                                                                                                                                                          |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aal5snap</b>   | Specifies AAL, an encapsulation type that supports Inverse Address Resolution Protocol (ARP). Logical link control/Subnetwork Access Protocol (LLC/SNAP) precedes the protocol datagram. |
| <b>group</b>      | (Optional) Specifies that a PPPoE profile is used by PPPoE sessions on the interface.                                                                                                    |
| <i>group-name</i> | (Optional) Specifies the PPPoE profile to be used by PPPoE sessions on the interface.                                                                                                    |

## Command Default

The global default encapsulation option is **aal5snap**.

## Command Modes

ATM VC configuration (for an ATM PVC or SVC)  
 Bundle configuration (for a VC bundle)  
 PVC range configuration (for an ATM PVC range)  
 PVC-in-range configuration (for an individual PVC within a PVC range)  
 VC-class configuration (for a VC class)

## Command History

| Release   | Modification                                                                                                                                                                                   |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.3T     | This command was introduced.                                                                                                                                                                   |
| 12.0(3)T  | This command was enhanced to provide encapsulation configuration for ATM VC bundles. The <b>aal5mux frame</b> and <b>aal5mux voice</b> keywords were added for the Cisco MC3810 series router. |
| 12.0(7)XK | Support for the <b>aal5mux voice</b> option was added to Cisco 3600 series routers.                                                                                                            |
| 12.0(7)T  | The <b>aal5mux fr-atm-srv</b> option was added for the Cisco MC3810 router. The <b>aal5mux frame</b> option was changed to <b>aal5mux frame-relay</b> .                                        |
| 12.1(1)XA | Support for the <b>aal2</b> option was added to the Cisco MC3810 router.                                                                                                                       |
| 12.1(3)T  | The <b>aal5auto</b> option was added to provide encapsulation configuration for PPP over ATM SVCs.                                                                                             |
| 12.1(5)XM | Support for the <b>aal2</b> option was added to the Cisco AS5300 access server and Cisco 3600 multiservice platforms.                                                                          |
| 12.1(5)T  | The <b>aal5ciscoppp</b> , <b>aal5mux</b> , and <b>aal5snap</b> options were made available in PVC range and PVC-in-range configuration modes.                                                  |
| 12.2(2)T  | This command was integrated into Cisco IOS Release 12.2(2)T.                                                                                                                                   |

| Release     | Modification                                                                                                                                                                                                                        |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.1(1)DC1  | The <b>aal5autoppp</b> option was introduced on the Cisco 6400 universal access concentrator.                                                                                                                                       |
| 12.2(4)T    | The <b>aal5autoppp</b> option was integrated into Cisco IOS Release 12.2(4)T.                                                                                                                                                       |
| 12.2(13)T   | The <b>apollo</b> , <b>vines</b> , and <b>xns</b> values were removed as options for the <i>protocol</i> argument because Apollo Domain, Banyan VINES, and Xerox Network Systems are no longer supported in the Cisco IOS software. |
| 12.2(15)T   | The <b>group</b> option was added.                                                                                                                                                                                                  |
| 12.3(7)XI3  | This command was integrated into Cisco IOS Release 12.3(7)XI3.                                                                                                                                                                      |
| 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                                                                                                                      |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                                                                     |
| 12.4(11)XW  | The <b>pppoe</b> and <b>bridge ieee8023</b> options were added.                                                                                                                                                                     |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                                                                      |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                                                                     |

### Usage Guidelines

Release 12.4(20)MR only supports aal5snap encapsulation.

### Examples

#### SNAP Encapsulation Example

The following example configures a bundle called “bundle1” for **aal5snap** encapsulation:

```
Router# configure terminal
Router(config)# int atm2/0
Router(config-if)# bundle bundle1
Router(config-if-atm-bundle)# encapsulation aal5snap
```

# ethernet cfm cc

To set parameters for continuity check messages (CCMs), use the **ethernet cfm cc** command in global configuration mode. To reset parameters to their default values, use the **no** form of this command.

**ethernet cfm cc level** { **any** | *level-id* | *level-id-level-id* | [,*level-id-level-id*] } { **vlan** { *vlan-id* | **any** | *vlan-id-vlan-id* | [,*vlan-id-vlan-id*] } } [**interval** *seconds*] [**loss-threshold** *num-msgs*]

**no ethernet cfm cc level** { **any** | *level-id* | *level-id-level-id* | [,*level-id-level-id*] } { **vlan** { *vlan-id* | **any** | *vlan-id-vlan-id* | [,*vlan-id-vlan-id*] } } [**interval** *seconds*] [**loss-threshold** *num-msgs*]

| Syntax Description            |  |                                                                                                                                                                                                                                                           |
|-------------------------------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>level</b>                  |  | Indicates a maintenance level for the configuration.                                                                                                                                                                                                      |
| <b>any</b>                    |  | Indicates that all levels are to be configured.                                                                                                                                                                                                           |
| <i>level-id</i>               |  | Integer from 0 to 7 that identifies a maintenance level.                                                                                                                                                                                                  |
| <i>level-id-level-id</i>      |  | Integers from 0 to 7 that define a range of levels to be configured. The hyphen is required to separate starting and ending values that define the range.                                                                                                 |
| [, <i>level-id-level-id</i> ] |  | (Optional) Integers from 0 to 7 that define a list of ranges to be configured. The comma must be entered to separate ranges. The hyphen is required to separate starting and ending values that are used to define each range of levels to be configured. |
| <b>vlan</b>                   |  | Indicates a VLAN for configuration.                                                                                                                                                                                                                       |
| <i>vlan-id</i>                |  | Integer from 1 to 4094 that identifies a VLAN to be configured.                                                                                                                                                                                           |
| <b>any</b>                    |  | Indicates that all VLANs are to be configured.                                                                                                                                                                                                            |
| <i>vlan-id-vlan-id</i>        |  | Integers from 1 to 4094 that define a range of VLANs to be configured. The hyphen is required to separate starting and ending values that are used to define the range.                                                                                   |
| [, <i>vlan-id-vlan-id</i> ]   |  | (Optional) Integers from 1 to 4094 that define a list of VLAN ranges to be configured. The comma must be entered to separate ranges. The hyphen is required to separate starting and ending values that are used to define each range of VLANs.           |
| <b>interval</b>               |  | (Optional) Specifies, in seconds, the time between CCM transmissions.                                                                                                                                                                                     |
| <i>seconds</i>                |  | (Optional) Integer value in the range of 10 to 65535. The default is 30.                                                                                                                                                                                  |
| <b>loss-threshold</b>         |  | (Optional) Indicates the maximum number of CCMs that can be missed before declaring that a maintenance endpoint (MEP) is down.                                                                                                                            |
| <i>num-msgs</i>               |  | (Optional) Integer in the range of 2 to 255 that specifies the maximum number of CCMs that can be lost before a MEP is declared down. The default is 2.                                                                                                   |

**Command Default** For all maintenance levels and VLANs configured on a device, the interval is 30 seconds and the loss-threshold is 2.

**Command Modes** Global configuration (config)

**Command History**

| Release     | Modification                                                                                                                                                                  |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(33)SRA | This command was introduced.                                                                                                                                                  |
| 12.4(11)T   | This command was integrated into Cisco IOS Release 12.4(11)T.                                                                                                                 |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH.                                                                                                               |
| 12.2(33)SRD | The <b>evc</b> keyword and <i>evc-name</i> argument were added on the Cisco 7600 Series Route Switch Processor 720 (RSP 720) and the Cisco 7600 Series Supervisor Engine 720. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not support the <b>evc</b> parameter.                                                       |

**Usage Guidelines**

The **ethernet cfm cc** command is used to set parameters for generating and receiving CCMs in one of the following ways:

- Globally (per device)
- For a maintenance domain
- For a particular customer service instance (CSI)
- For a combination of maintenance domain and CSI

When the **ethernet cfm cc** command is issued, the system may perform optimizations by concatenating possible ranges, and the configuration may not go through nonvolatile generation (NVGEN) as it was originally entered.

If you configure the **ethernet cfm cc** command with the default values for interval and loss threshold, these parameters are not displayed after NVGEN. If you configure the command with at least one parameter not at the default value, all parameters are displayed.

An EVC is an association of two or more user network interfaces (UNIs).

**Note**

This command is not supported in the Connectivity Fault Management 802.1ag Standard (CFM IEEE).

**Examples**

The following example shows how to configure an Ethernet CFM level ID of 5 for all VLANs, with messages transmitted every 30 seconds and a remote MEP declared down after two messages are missed. Note that the interval and loss-threshold parameters are configured for the default values and do not display after NVGEN.

```
Router(config)# ethernet cfm cc level 5 vlan any interval 30 loss-threshold 2
(NVGEN)ethernet cfm cc level 5 vlan any
```

The following example shows how to configure an Ethernet CFM level ID of 5 for all VLANs, with messages transmitted every 1000 seconds and a remote MEP declared down after two messages (the default value) are missed:

```
Router(config)# ethernet cfm cc level 5 vlan any interval 1000 loss-threshold 2
(NVGEN)ethernet cfm cc level 5 vlan any interval 1000
```

The following example shows how to configure an Ethernet CFM level ID of 5 for all VLANs, with messages transmitted every 1000 seconds and a remote MEP declared down after 7 messages are missed (neither value is a default value):

```
Router(config)# ethernet cfm cc level 5 vlan any interval 1000 loss-threshold 7
(NVGEN)ethernet cfm cc level 5 vlan any interval 1000 loss-threshold 7
```

The following example shows how to configure Ethernet CFM for multiple levels for VLANs 100 to 200 with messages transmitted every 50 seconds and a remote MEP declared down after 5 messages are missed (neither value is a default value):

```
Router(config)# ethernet cfm cc level 1-5 vlan 100-200 interval 50 loss-threshold 5
Router(config)# no ethernet cfm cc level 2-3 vlan 50-150 interval 50 loss-threshold 5
(NVGEN)ethernet cfm cc level 2-3 vlan 151-200 interval 50 loss-threshold 5
        ethernet cfm cc level 1,4-5 vlan 100-200 interval 50 loss-threshold 5
```

# ethernet cfm cc enable level vlan

Use the **ethernet cfm cc enable level vlan** command in global configuration mode to globally enable transmission of continuity check messages (CCMs). To disable transmission of CCMs, use the **no** form of this command.

**ethernet cfm cc enable level** { **any** | *level-id* | ,*level-id* | *level-id-level-id* | ,*level-id-level-id* }  
**vlan** { **any** | *vlan-id* | ,*vlan-id* | *vlan-id-vlan-id* | ,*vlan-id-vlan-id* }

**no ethernet cfm cc enable level** { **any** | *level-id* | ,*level-id* | *level-id-level-id* | ,*level-id-level-id* }  
**vlan** { **any** | *vlan-id* | ,*vlan-id* | *vlan-id-vlan-id* | ,*vlan-id-vlan-id* }

## Syntax Description

|                            |                                                                                                                                                                                                                                          |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>any</b>                 | Enables CCMs for all levels.                                                                                                                                                                                                             |
| <i>level-id</i>            | Integer from 0 to 7 that identifies a maintenance level.                                                                                                                                                                                 |
| , <i>level-id</i>          | Integers from 0 to 7, separated by commas, that list levels to be enabled.                                                                                                                                                               |
| <i>level-id-level-id</i>   | Integers from 0 to 7 that define a range of levels to be enabled. The hyphen is required to separate starting and ending values that define the range.                                                                                   |
| , <i>level-id-level-id</i> | Integers from 0 to 7 that define a list of ranges to be enabled. The comma must be entered to separate ranges. The hyphen is required to separate starting and ending values that are used to define each range of levels to be enabled. |
| <b>any</b>                 | Indicates all VLANs are to be configured.                                                                                                                                                                                                |
| <i>vlan-id</i>             | Integer from 1 to 4094 that identifies a VLAN to be configured.                                                                                                                                                                          |
| , <i>vlan-id</i>           | Integers from 1 to 4094, separated by commas, that list VLANs to be configured.                                                                                                                                                          |
| <i>vlan-id-vlan-id</i>     | Integers from 1 to 4094 that define a range of VLANs to be configured. The hyphen is required to separate starting and ending values that are used to define the range.                                                                  |
| , <i>vlan-id-vlan-id</i>   | Integers from 1 to 4094 that define a list of VLAN ranges to be configured. The comma must be entered to separate ranges. The hyphen is required to separate starting and ending values that are used to define each range of VLANs.     |

## Command Default

No CCMs are transmitted.

## Command Modes

Global configuration (config)

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(33)SRA | This command was introduced.                                    |
| 12.4(11)T   | This command was integrated into Cisco IOS Release 12.4(11)T.   |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

---

**Usage Guidelines**

Use the **ethernet cfm cc enable level vlan** command to enable transmission of CCMs in one of the following ways:

- Globally (per device)
- For a particular level
- For a particular VLAN
- For a combination of level and VLAN

The syntax of the **ethernet cfm cc enable level vlan** command as entered in the CLI and the format of the command as shown in the configuration can be different. For example, if you enter:

```
Router(config)# ethernet cfm cc enable level 1,2,3,4,5 vlan 100,101,102,103,105
```

The configuration shows the following:

```
ethernet cfm cc enable level 1-5 vlan 100-103,105
```

To shorten the length of the command, you enter the command in the second format.

---

**Examples**

The following examples show how this command functions:

The command already configured is:

```
ethernet cfm cc enable level 1-5 vlan 100-200
```

You configure this new command:

```
Router(config)# no ethernet cfm cc enable level 2-3 vlan 50-150
```

The following commands are generated as a result of the command you have just configured. Note that these commands are different from the command you entered.

```
ethernet cfm cc enable level 1,4-5 vlan 100-200  
ethernet cfm cc enable level 2-3 vlan 151-200
```

# ethernet cfm domain level

To define a connectivity fault management (CFM) maintenance domain at a particular maintenance level and put the command-line interface (CLI) into Ethernet CFM configuration mode, use the **ethernet cfm domain level** command in global configuration mode. To remove the CFM domain at the specified level, use the **no** form of this command.

**ethernet cfm domain** *domain-name* **level** *level-id* [**direction outward**]

**no ethernet cfm domain** *domain-name* **level** *level-id*

## Syntax Description

|                          |                                                                                                                                                                          |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>domain-name</i>       | String of a maximum of 154 characters that identifies the domain.                                                                                                        |
| <i>level-id</i>          | Integer from 0 to 7 that identifies the maintenance level.                                                                                                               |
| <b>direction outward</b> | (Optional) Specifies the domain direction as outward (toward the wire). The default direction is inward.                                                                 |
| <b>Note</b>              | The outward keyword is supported only in Cisco IOS Release 12.4(11)T and later releases. This keyword is not supported in Cisco IOS Release 12.2(33)SXH or 12.2(33)SXI2. |

## Command Default

No maintenance domains are assigned to maintenance levels if this command is not issued.

## Command Modes

Global configuration (config)

## Command History

| Release      | Modification                                                                                                    |
|--------------|-----------------------------------------------------------------------------------------------------------------|
| 12.2(33)SRA  | This command was introduced.                                                                                    |
| 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T. The <b>direction outward</b> keywords were added. |
| 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.                                                 |
| 12.2(33)SXI2 | This command was integrated into Cisco IOS Release 12.2(33)SXI2.                                                |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                 |

## Usage Guidelines

When a router is in Ethernet CFM configuration mode, parameters specific to a maintenance domain can be set. Several domains, with different names, can be configured at the same maintenance level; however, a single domain cannot be associated with multiple levels.

In CFM IEEE, if a domain name has more than 43 characters, a warning message is displayed notifying that the maintenance domain ID (MDID) is truncated to 43 characters in continuity check messages (CCMs) if “id <fmt> <MDID>” is not configured.

When this command places the CLI in Ethernet configuration mode, in CFM D1 the mode prompt is “config-ether-cfm” and in CFM IEEE the mode prompt is “config-ecfm.”



## Examples

The following example shows how to define an outward facing domain named domain1 at level 6 and that the CLI mode changes to Ethernet CFM configuration mode:

```
Router(config)# ethernet cfm domain domain1 level 6 direction outward
Router(config-ether-cfm)#
```

The following example shows how to define a domain named cust10 at level 5 and also shows the Ethernet CFM configuration mode prompt that is displayed in the CFM IEEE Standard implementation:

```
Router(config)# ethernet cfm domain cust10 level 5
Router(config-ether-cfm)#
```

## Related Commands

| Command                                           | Description                                                           |
|---------------------------------------------------|-----------------------------------------------------------------------|
| <b>show ethernet cfm domain</b>                   | Displays information about maintenance points configured on a device. |
| <b>show ethernet cfm maintenance-points local</b> | Displays information about maintenance points configured on a device. |

# ethernet cfm enable

To enable connectivity fault management (CFM) processing globally on a device, use the **ethernet cfm enable** command in global configuration mode. To disable CFM processing globally on a device, use the **no** form of this command.

- ethernet cfm enable**
- no ethernet cfm enable**

Syntax Description

This command has no arguments or keywords.

Command Default

Ethernet CFM is disabled.

Command Modes

Global configuration (config)

Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(33)SRA | This command was introduced.                                    |
| 12.4(11)T   | This command was integrated into Cisco IOS Release 12.4(11)T.   |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

Usage Guidelines

Ethernet CFM is disabled by default and must be enabled explicitly. When CFM is configured, hardware resources (for example, port-ASIC match-registers) are allocated for CFM.

Examples

The following example shows how to enable CFM processing globally on a device:

```
Router(config)# ethernet cfm enable
```

# ethernet cfm enable (interface)

To enable connectivity fault management (CFM) processing on an interface, use the **ethernet cfm enable** command in interface configuration mode. To disable CFM processing on an interface, use the **no** form of this command.

**ethernet cfm enable**

**no ethernet cfm enable**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Ethernet CFM is enabled.

**Command Modes** Interface configuration (config-if)

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(33)SRA | This command was introduced.                                    |
|                 | 12.4(11)T   | This command was integrated into Cisco IOS Release 12.4(11)T.   |
|                 | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** Ethernet CFM is enabled by default on an interface and must be disabled explicitly. When CFM is disabled on an interface, hardware resources (for example, port-ASIC match-registers) are released for that interface.

This command is mutually exclusive of maintenance intermediate point (MIP) and maintenance end point (MEP) configuration commands. The interface must be enabled before any MEPs or MIPs can be configured. Similarly, disabling a port that has MIPs or MEPs configured is not allowed. The user must first unconfigure the maintenance points.

When CFM processing is disabled on an interface, all CFM frames that arrive at that interface are forwarded as normal data traffic, and are not processed by the CPU.

**Examples** The following example shows how to disable and then enable CFM processing on an interface:

```
Router(config-if)# no ethernet cfm enable
Router(config-if)# ethernet cfm enable
```

# ethernet cfm logging

To enable Ethernet Connectivity Fault Management (CFM) syslog messages, use the **ethernet cfm logging** command in global configuration mode. To disable CFM syslog messages, use the **no** form of this command.



Note

Release 12.2(33)MRA supports the Draft 1.0 version of Ethernet CFM; it does not support the IEEE 802.1ag-2007 version.

Cisco pre-Standard CFM Draft 1 (CFM D1)

```
ethernet cfm logging [ais | alarm { cisco | ieee}]

no ethernet cfm logging [ais | alarm { cisco | ieee}]
```

CFM IEEE 802.1ag Standard (CFM IEEE)

```
ethernet cfm logging [ais | alarm { cisco | ieee} | lck]

no ethernet cfm logging [ais | alarm { cisco | ieee} | lck]
```

Syntax Description

|       |                                                                                               |
|-------|-----------------------------------------------------------------------------------------------|
| ais   | (Optional) Enables syslog messages specific to the CFM Alarm Indication Signal (AIS) feature. |
| alarm | (Optional) Specifies an alarm.                                                                |
| cisco | (Optional) Enables alarm syslog messages for Cisco MIBs.                                      |
| ieee  | (Optional) Enables alarm syslog messages for IEEE MIBs for all VLAN services.                 |
| lck   | (Optional) Enables syslog messages specific to the CFM Locked Signal function (LCK).          |

Command Default

CFM logging is not enabled.

Command Modes

Global configuration (config)

Command History

| Release      | Modification                                                     |
|--------------|------------------------------------------------------------------|
| 12.2(33)SRD  | This command was introduced.                                     |
| 12.2(33)SX12 | This command was integrated into Cisco IOS Release 12.2(33)SX12. |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.  |

Examples

The following example shows how to enable all Ethernet CFM syslog messages:

```
Router(config)# ethernet cfm logging
```

The following example shows how to enable all alarm syslog messages for Cisco MIBs:

```
Router(config)# ethernet cfm logging alarm cisco
```

The following example shows how to enable syslog messages specific to the CFM AIS feature:

```
Router(config)# ethernet cfm logging ais
```

# ethernet cfm mep crosscheck

To enable cross-checking between the list of configured remote maintenance endpoints (MEPs) of a domain and MEPs learned through continuity check messages (CCMs), use the **ethernet cfm mep crosscheck** command in privileged EXEC mode. To disable cross-checking, use the **ethernet cfm mep crosscheck disable** command.



## Note

Release 12.2(33)MRA supports the Draft 1.0 version of Ethernet CFM; it does not support the IEEE 802.1ag-2007 version.

### Cisco pre-Standard Connectivity Fault Management Draft 1 (CFM D1)

```
ethernet cfm mep crosscheck {enable | disable} level {level-id | level-id-level-id
[,level-id-level-id]} {vlan {vlan-id | any | vlan-id-vlan-id [,vlan-id-vlan-id]}}
```

### CFM IEEE 802.1ag Standard (CFM IEEE)

```
ethernet cfm mep crosscheck {enable | disable} domain domain-name {port | vlan {vlan-id |
vlan-id-vlan-id | ,vlan-id-vlan-id}}
```

## Syntax Description

|                           |                                                                                                                                                                                                                  |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>enable</b>             | Indicates that cross-checking occurs.                                                                                                                                                                            |
| <b>disable</b>            | Indicates that cross-checking does not occur.                                                                                                                                                                    |
| <b>level</b>              | Indicates a maintenance level for configuration.                                                                                                                                                                 |
| <i>level-id</i>           | Integer from 0 to 7 that identifies the maintenance level.                                                                                                                                                       |
| <i>level-id-level-id</i>  | Integer values from 0 to 7. The hyphen is required to separate starting and ending level ID values that are used to define the range of IDs.                                                                     |
| <i>,level-id-level-id</i> | (Optional) Integer values from 0 to 7. The comma must be entered to separate level ID ranges. The hyphen is required to separate starting and ending level ID values that are used to define each range of IDs.  |
| <b>vlan</b>               | Indicates a VLAN for cross-checking.                                                                                                                                                                             |
| <i>vlan-id</i>            | Integer from 1 to 4094 that identifies the VLAN.                                                                                                                                                                 |
| <b>any</b>                | Indicates all VLANs are to be configured. <ul style="list-style-type: none"> <li>This option is supported only in CFM D1.</li> </ul>                                                                             |
| <i>vlan-id-vlan-id</i>    | Integer values from 1 to 4094. The hyphen is required to separate starting and ending VLAN ID values that are used to define a range of IDs.                                                                     |
| <i>,vlan-id-vlan-id</i>   | (Optional) Integer values from 1 to 4094. The comma must be entered to separate VLAN ID ranges. The hyphen is required to separate starting and ending VLAN ID values that are used to define each range of IDs. |
| <b>domain</b>             | Specifies a maintenance domain.                                                                                                                                                                                  |
| <i>domain-name</i>        | String of a maximum of 154 characters that identifies the maintenance domain.                                                                                                                                    |
| <b>port</b>               | Specifies a DOWN service direction with no VLAN associations (untagged).                                                                                                                                         |

## Command Modes

Privileged EXEC (#)

**Command History**

| Release      | Modification                                                                                                                                                                  |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(33)SRA  | This command was introduced.                                                                                                                                                  |
| 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T.                                                                                                                 |
| 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.                                                                                                               |
| 12.2(33)SRD  | The <b>evc</b> keyword and <i>evc-name</i> argument were added on the Cisco 7600 Series Route Switch Processor 720 (RSP 720) and the Cisco 7600 Series Supervisor Engine 720. |
| 12.2(33)SX12 | This command was integrated into Cisco IOS Release 12.2(33)SX12.                                                                                                              |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not support the <b>evc</b> parameter.                                                       |

**Usage Guidelines**

Before you issue this command, you must configure a static list of MEPs using the **mep crosscheck mpid vlan** command. To enable cross-checking after a device has booted up, you must issue the **ethernet cfm mep crosscheck enable** command.

A **no** form of this command does not exist. Cross-checking is disabled when you issue the command with the **disable** keyword.

In CFM IEEE, if a domain name has more than 43 characters, a warning message is displayed notifying that the maintenance domain ID (MDID) is truncated to 43 characters in continuity check messages (CCMs) if “id <fmt> <MDID>” is not configured.

To view the results of a cross-check operation, use the **show ethernet cfm maintenance-points remote crosscheck** command. To view errors in the cross-check operation, use the **show ethernet cfm errors** command. Both commands are used in privileged EXEC mode.

Traps are generated after a cross-check operation is completed if cross-check traps are already enabled and, if as the result of the cross-check operation, a condition warrants a trap to be sent.

An EVC is an association of two or more user network interfaces (UNIs). EVCs are not supported in Cisco IOS Release 12.2(33)SX12.

**Examples**

The following example shows how to enable an Ethernet CFM MEP cross-check on a port MEP in CFM IEEE:

```
Router# ethernet cfm mep crosscheck enable domain customerA port
```

The following example shows how to enable an Ethernet CFM MEP cross-check in CFM D1 at level 2 for VLAN IDs in the range of 3000 to 3375:

```
Router# ethernet cfm mep crosscheck enable level 2 vlan 3000-3375
```

**Related Commands**

| Command                                                       | Description                                                                                                                  |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>mep crosscheck mpid vlan</b>                               | Statically defines a remote MEP within a maintenance domain.                                                                 |
| <b>show ethernet cfm errors</b>                               | Displays CFM continuity check error conditions logged on a device since it was last reset or since the log was last cleared. |
| <b>show ethernet cfm maintenance-points remote crosscheck</b> | Displays detailed information about remote MEPs in the cross-check list that were statically configured.                     |

# ethernet cfm mep crosscheck start-delay

To configure the maximum amount of time that a device waits for remote maintenance endpoints (MEPs) to come up before the cross-check operation is started, use the **ethernet cfm mep crosscheck start-delay** command in global configuration mode. To restore the default number of seconds a device waits, use the **no** form of this command.

- ethernet cfm mep crosscheck start-delay *delay*
- no ethernet cfm mep crosscheck start-delay *delay*

|                    |              |                                                                                                                                                              |
|--------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>delay</i> | Integer from 1 to 65535 that specifies the number of seconds a device waits for remote MEPs to come up before the cross-check is started. The default is 30. |
|--------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                                   |
|-----------------|-------------------------------------------------------------------|
| Command Default | The start delay interval is enabled with a default of 30 seconds. |
|-----------------|-------------------------------------------------------------------|

|               |                               |
|---------------|-------------------------------|
| Command Modes | Global configuration (config) |
|---------------|-------------------------------|

|                 |              |                                                                  |
|-----------------|--------------|------------------------------------------------------------------|
| Command History | Release      | Modification                                                     |
|                 | 12.2(33)SRA  | This command was introduced.                                     |
|                 | 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T.    |
|                 | 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.  |
|                 | 12.2(33)SXI2 | This command was integrated into Cisco IOS Release 12.2(33)SXI2. |
|                 | 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.  |

|                  |                                                                                                                                                                                                                                                                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usage Guidelines | <p>If continuity check intervals in your network are greater than 30 seconds (the delay default), you must configure the start-delay to match the greatest interval to avoid unnecessary traps.</p> <p>When the default value is configured, “ethernet cfm mep crosscheck start-delay 30” is displayed when the <b>show running all</b> command is issued.</p> |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|          |                                                                                                                                                                                                                                                       |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Examples | <p>The following example shows how to set the maximum number of seconds that a device waits for remote MEPs to come up before the cross-check operation is started to 700:</p> <pre>Router(config)# ethernet cfm mep crosscheck start-delay 700</pre> |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                  |                  |                                                      |
|------------------|------------------|------------------------------------------------------|
| Related Commands | Command          | Description                                          |
|                  | show running all | Shows the running configuration with default values. |



# ethernet cfm mep domain mpid

To set a port as internal to a maintenance domain and define it as a maintenance endpoint (MEP), use the **ethernet cfm mep domain mpid** command in interface configuration mode. Also, use this command to place the command-line interface (CLI) in Ethernet connectivity fault management (CFM) MEP configuration mode (config-if-ecfm-mep). To restore the default configuration of the port, use the **no** form of this command.

**ethernet cfm mep domain** *domain-name* **mpid** *mpid* {**port** | **vlan** *vlan-id*}

**no ethernet cfm mep domain** *domain-name* **mpid** *mpid* {**port** | **vlan** *vlan-id*}

## Syntax Description

|                    |                                                                            |
|--------------------|----------------------------------------------------------------------------|
| <i>domain-name</i> | String of a maximum of 154 characters.                                     |
| <i>mpid</i>        | Integer from 1 to 8191 that identifies the MEP.                            |
| <b>port</b>        | Configures the DOWN service direction with no VLAN association (untagged). |
| <b>vlan</b>        | Configures a VLAN.                                                         |
| <i>vlan-id</i>     | Integer from 1 to 4094 that identifies a VLAN.                             |

## Command Default

This command is disabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release      | Modification                                                    |
|--------------|-----------------------------------------------------------------|
| 12.2(33)SX12 | This command was introduced.                                    |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

A single interface may belong to multiple domains, meaning that you can issue multiple instances of the **ethernet cfm mep domain mpid** command for different domains.

If a specified domain has not been configured, an error message is displayed and the command is rejected.

If an interface is manually provisioned to have a maintenance intermediate point (MIP) at a certain maintenance level and you attempt to configure it as a MEP for a VLAN on the same or a higher level, an error message is displayed and the command is rejected.

If the VLAN for which a MEP is configured is removed from an interface, the MEP configuration is also removed; the VLAN and the definition of the MEP are interrelated.

If a domain name has more than 43 characters, a warning message is displayed notifying that the maintenance domain ID (MDID) is truncated to 43 characters in continuity check messages (CCMs) if “id <fmt> <MDID>” is not configured.

---

**Examples**

The following example shows how to set a port as internal to a maintenance domain, define it as a maintenance endpoint (MEP), and configure VLAN 17:

```
Router(config)# interface ethernet 0/1  
Router(config-if)# ethernet cfm mep domain CustomerB mpid 5 vlan 17  
Router(config-if)#
```

# ethernet cfm mep level mpid vlan

To set an interface as a domain boundary (edge), define it as a maintenance endpoint (MEP), and set direction for the MEP, use the **ethernet cfm mep level mpid vlan** command in interface configuration mode. To restore the default configuration of the interface, use the **no** form of this command.

**ethernet cfm mep level** *level-id* [**inward** | **outward domain** *domain-name*] **mpid id vlan** {**any** | *vlan-id* | ,*vlan-id* | *vlan-id-vlan-id* | ,*vlan-id-vlan-id*}

**no ethernet cfm mep level** *level-id* [**inward** | **outward domain** *domain-name*] **mpid id vlan** {**any** | *vlan-id* | ,*vlan-id* | *vlan-id-vlan-id* | ,*vlan-id-vlan-id*}

## Syntax Description

|                          |                                                                                                                                                                                                                                      |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>level-id</i>          | Integer from 0 to 7 that identifies the maintenance level at which the MEP is defined.                                                                                                                                               |
| <b>inward</b>            | (Optional) Indicates the direction of the MEP is toward the device. This is the default.                                                                                                                                             |
| <b>outward</b>           | (Optional) Sets an interface as outward (toward the wire).                                                                                                                                                                           |
| <b>domain</b>            | (Optional) Identifies the domain in which the MEP is configured.                                                                                                                                                                     |
| <i>domain-name</i>       | (Optional) String of a maximum of 154 characters that identifies the domain.                                                                                                                                                         |
| <i>id</i>                | Integer from 0 to 8191 that identifies the MEP.                                                                                                                                                                                      |
| <b>any</b>               | Indicates all VLANs are to be configured.                                                                                                                                                                                            |
| <i>vlan-id</i>           | Integer from 1 to 4094 that identifies a VLAN to be configured.                                                                                                                                                                      |
| , <i>vlan-id</i>         | Integers from 1 to 4094, separated by commas, that list VLANs to be configured.                                                                                                                                                      |
| <i>vlan-id-vlan-id</i>   | Integers from 1 to 4094 that define a range of VLANs to be configured. The hyphen is required to separate starting and ending values that are used to define the range.                                                              |
| , <i>vlan-id-vlan-id</i> | Integers from 1 to 4094 that define a list of VLAN ranges to be configured. The comma must be entered to separate ranges. The hyphen is required to separate starting and ending values that are used to define each range of VLANs. |

## Command Default

No MEPs are configured until this command is issued.

## Command Modes

Interface configuration (config-if)

## Command History

| Release     | Modification                                                                                                                                                       |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(33)SRA | This command was introduced.                                                                                                                                       |
| 12.4(11)T   | This command was integrated into Cisco IOS Release 12.4(11)T.<br><br>The <b>outward</b> and <b>domain</b> keywords and the <i>domain-name</i> argument were added. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH.                                                                                                    |

| Release     | Modification                                                                                        |
|-------------|-----------------------------------------------------------------------------------------------------|
| 12.2(33)SRD | This command was added to support outward facing MEPs on switch ports on Cisco 7600 series routers. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                     |

### Usage Guidelines

Following is the order in which you must configure Ethernet connectivity fault management (CFM) elements:

1. Domain at the same level as the MEP to be configured
2. Service within the domain
3. Maintenance intermediate point (MIP) at a level higher than the MEP if the domain is not an outward domain
4. MEP

If you do not configure elements in this sequence, the **ethernet cfm mep level mpid vlan** command fails. An exception is at maintenance level 7, where configuring a MIP on the interface before you configure a MEP is not required. Configuring a MIP on an interface also is not required when you are configuring an outward facing MEP.

A single interface may belong to multiple domains, which means you can issue multiple instances of the **ethernet cfm mep level mpid vlan** command for different domains and for different VLANs.

More than one domain can be configured at a single level. The level plus VLAN indicates the domain to which the MEP belongs.

You can configure a single MEP, a list of MEPs, or a range of MEPs so that there is one MEP per VLAN and all MEPs share the same level, direction, and maintenance endpoint ID (MPID).

If the direction of the MEP is not stated, the default is inward facing (toward the Bridge). When you specify an outward MEP, you must provide a domain name. If the specified domain has not been configured or if the specified domain has not been tagged as outward, an error message displays and the command is rejected.

All MEPs and MIPs must be removed from an interface before MEPs at level 7 can be configured. Also, when you remove MEP configurations at Level 7, you should first remove all lower level MEPs. If you try to configure a MEP on an interface with a level higher than the MIP level, the command is rejected and an error message is displayed.

If an interface is provisioned to be a MIP for a certain maintenance level and you try to configure the interface as an inward MEP for a VLAN at the same level, the command is rejected and an error message displays. If a VLAN for which a MEP is configured is removed from an interface, the MEP configuration remains, but the MEP is inactive and does not transmit or receive messages because the definition of the MEP is associated with the VLAN.

### Examples

The following example shows how to set interface Ethernet 0/1 as a domain boundary and define it as a MEP at level 5, with a MPID of 5 on VLAN 101, and then issue the **show ethernet cfm maintenance-points local** command to display the list of configured MEPs in the device:

```
Router(config)# interface ethernet 0/1
Router(config-if)# ethernet cfm mep level 5 mpid 5 vlan 101
Router(config-if)# Ctrl-Z
Router(config)# show ethernet cfm maintenance-points local
```

The following example shows how to set interface Ethernet 0/1 as outward for maintenance domain domain1 and define it as a MEP at level 5 with the MEP ID 700 on VLAN 5:

```
Router(config)# interface ethernet 0/1
Router(config-if)# ethernet cfm mep level 5 outward domain domain1 mpid 700 vlan 5
```

The following example shows how to set interface Ethernet 5/0 as a domain boundary and define it as a MEP at level 7, with a MPID of 3001 on VLAN 100 on a switch port:

```
Router(config)# interface ethernet 5/0
Router(config-if)# switchport
Router(config-if)# switchport mode trunk
Router(config-if)# ethernet cfm mep level 7 outward domain CUSTOMER mpid 3001 vlan 100
```

The following example shows how to set interface Ethernet 5/0 as a domain boundary and define it as a MEP at level 7, with a MPID of 3001 on VLAN 100 on a routed port:

```
Router(config)# interface ethernet 5/0
Router(config-if)# ethernet cfm mep level 7 outward domain CUSTOMER mpid 3001 vlan 100
!
Router(config-if)# interface Ethernet5/0.100
Router(config-if)# encapsulation dot1Q 100
```

## Related Commands

| Command                                           | Description                                                                               |
|---------------------------------------------------|-------------------------------------------------------------------------------------------|
| <b>ethernet cfm domain</b>                        | Defines a CFM domain at a specified maintenance level.                                    |
| <b>ethernet cfm mip level</b>                     | Provisions a MIP at a specified maintenance level on an interface.                        |
| <b>service vlan</b>                               | Sets a universally unique ID for a customer service instance within a maintenance domain. |
| <b>show ethernet cfm maintenance-points local</b> | Displays maintenance points configured on a device.                                       |

# ethernet cfm mip level

To provision a maintenance intermediate point (MIP) at a specified maintenance level on an interface, use the **ethernet cfm mip level** command in interface configuration mode. To restore the default configuration of the interface, use the **no** form of this command.



**Note**

Release 12.2(33)MRA supports the Draft 1.0 version of Ethernet CFM; it does not support the IEEE 802.1ag-2007 version.

**Cisco pre-Standard Connectivity Fault Management Draft 1 (CFM D1)**

**ethernet cfm mip level** *level-id*

**no ethernet cfm mip level** *level-id*

**CFM IEEE 802.1ag Standard (CFM IEEE)**

**ethernet cfm mip level** *level-id* [**vlan** {*vlan-id* | *vlan-id-vlan-id* | ,*vlan-id-vlan-id*}]

**no ethernet cfm mip level** *level-id* [**vlan** {*vlan-id* | *vlan-id-vlan-id* | ,*vlan-id-vlan-id*}]

**Syntax Description**

|                          |                                                                                                                                                                                                                                                                  |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>level-id</i>          | Integer from 0 to 7 that specifies the maintenance levels at which MIPs can be defined.                                                                                                                                                                          |
| <b>vlan</b>              | (Optional) Indicates a VLAN for configuration.                                                                                                                                                                                                                   |
| <i>vlan-id</i>           | (Optional) Integer from 1 to 4094 that identifies the VLAN to be configured.                                                                                                                                                                                     |
| <i>vlan-id-vlan-id</i>   | (Optional) Integers from 1 to 4094 that define a valid range of VLANs to be configured. <ul style="list-style-type: none"><li>The hyphen is required to separate the starting and ending VLAN ID values that are used to define the range of VLAN IDs.</li></ul> |
| , <i>vlan-id-vlan-id</i> | (Optional) Integers from 1 to 4094 that define a valid range of VLANs to be configured. <ul style="list-style-type: none"><li>The comma is required to separate VLAN ranges.</li></ul>                                                                           |

**Command Default**

No MIPs are configured.

**Command Modes**

Interface configuration (config-if)

**Command History**

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(33)SRA | This command was introduced.                                    |
| 12.4(11)T   | This command was integrated into Cisco IOS Release 12.4(11)T.   |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

| Release      | Modification                                                     |
|--------------|------------------------------------------------------------------|
| 12.2(33)SX12 | This command was integrated into Cisco IOS Release 12.2(33)SX12. |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.  |

### Usage Guidelines

If you do not configure a VLAN, this command creates MIPs for all VLANs on an interface.

In the CFM D1 implementation, you must first configure a domain using the **ethernet cfm domain** command at the level you want to configure the MIP; otherwise, the **ethernet cfm mip level** command is rejected. In the CFM IEEE implementation, preconfiguring a domain is not required.

You cannot configure a MIP at a level lower than the level of already configured maintenance endpoints (MEPs) on an interface.

Configuring a MIP using this command is known as a manual MIP and has precedence over the **mip auto-create** command.

### Examples

The following example shows how to provision a MIP at maintenance level 5 and then issue the **show ethernet cfm maintenance-points local** command to display the list of configured MIPs in the device:

```
Router(config-if)# ethernet cfm mip level 5
Router(config-if)# Ctrl-Z
Router# show ethernet cfm maintenance-points local
```

### Related Commands

| Command                                           | Description                                                            |
|---------------------------------------------------|------------------------------------------------------------------------|
| <b>ethernet cfm domain</b>                        | Defines a CFM domain.                                                  |
| <b>mip auto-create</b>                            | Enables the automatic creation of a MIP at a maintenance domain level. |
| <b>show ethernet cfm maintenance-points local</b> | Displays information about maintenance points configured on a device.  |

# ethernet cfm traceroute cache

To enable caching of Ethernet connectivity fault management (CFM) data learned through traceroute messages, use the **ethernet cfm traceroute cache** command in global configuration mode. To disable caching, use the **no** form of this command.

- ethernet cfm traceroute cache**
- no ethernet cfm traceroute cache**

Syntax Description

This command has no arguments or keywords.

Command Default

Caching is disabled.

Command Modes

Global configuration (config)

| Command History | Release      | Modification                                                     |
|-----------------|--------------|------------------------------------------------------------------|
|                 | 12.2(33)SRA  | This command was introduced.                                     |
|                 | 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T.    |
|                 | 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.  |
|                 | 12.2(33)SXI2 | This command was integrated into Cisco IOS Release 12.2(33)SXI2. |
|                 | 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.  |

Usage Guidelines

Setting a traceroute cache allows you to store the results of traceroute operations initiated on the device.

Examples

The following example shows how to enable Ethernet CFM traceroute cache:

```
Router(config)# ethernet cfm traceroute cache
```

| Related Commands | ethernet cfm traceroute cache hold-time | Sets a maximum time that Ethernet CFM traceroute cache entries are retained. |
|------------------|-----------------------------------------|------------------------------------------------------------------------------|
|                  | ethernet cfm traceroute cache size      | Sets a maximum number for entries in an Ethernet CFM traceroute cache table. |



# ethernet cfm traceroute cache hold-time

To set the time that Ethernet connectivity fault management (CFM) traceroute cache entries are retained, use the **ethernet cfm traceroute cache hold-time** command in global configuration mode. To remove the configured time, use the **no** form of this command.

**ethernet cfm traceroute cache hold-time** *minutes*

**no ethernet cfm traceroute cache hold-time**

## Syntax Description

|                |                                                                                                                              |
|----------------|------------------------------------------------------------------------------------------------------------------------------|
| <i>minutes</i> | Integer in the range of 1 to 65535 that specifies the number of minutes that cache entries are retained. The default is 100. |
|----------------|------------------------------------------------------------------------------------------------------------------------------|

## Command Default

Entries are retained for 100 minutes.

## Command Modes

Global configuration (config)

## Command History

| Release      | Modification                                                     |
|--------------|------------------------------------------------------------------|
| 12.2(33)SRA  | This command was introduced.                                     |
| 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T.    |
| 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.  |
| 12.2(33)SX12 | This command was integrated into Cisco IOS Release 12.2(33)SX12. |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.  |

## Usage Guidelines

Before you can issue this command, you must have enabled traceroute caching using the **ethernet cfm traceroute cache** command.

If traceroute cache is enabled and not empty and you change the hold time to less than the currently configured time, the change is rejected. You are prompted to clean up the table before the new hold time can be accepted. For example:

```
Router(config)# ethernet cfm traceroute cache hold-time 5
Please clean up the cache before setting smaller hold-time
current hold time = 100 Command Aborted.
Router(config)#
```

Output of the **show running all** command displays “ethernet cfm traceroute cache hold-time 100” when traceroute cache is enabled and the default value of 100 is configured.

## Examples

The following example shows how to set the retention time for entries in an Ethernet CFM traceroute cache table to 5 minutes:

```
Router(config)# ethernet cfm traceroute cache hold-time 5
```

|                         |                                           |                                                                              |
|-------------------------|-------------------------------------------|------------------------------------------------------------------------------|
| <b>Related Commands</b> | <b>ethernet cfm traceroute cache</b>      | Enables caching of Ethernet CFM data learned from traceroute messages.       |
|                         | <b>ethernet cfm traceroute cache size</b> | Sets a maximum number for entries in an Ethernet CFM traceroute cache table. |
|                         | <b>show running all</b>                   | Shows the running configuration with default values.                         |

# ethernet cfm traceroute cache size

To set a maximum size for the Ethernet connectivity fault management (CFM) traceroute cache table, use the **ethernet cfm traceroute cache size** command in global configuration mode. To remove the configured size, use the **no** form of this command.

**ethernet cfm traceroute cache size** *entries*

**no ethernet cfm traceroute cache size**

## Syntax Description

|                |                                                                                                                         |
|----------------|-------------------------------------------------------------------------------------------------------------------------|
| <i>entries</i> | Number of entries in the traceroute cache table, expressed as an integer in the range of 1 to 4095. The default is 100. |
|----------------|-------------------------------------------------------------------------------------------------------------------------|

## Command Default

If traceroute cache is enabled, traceroute replies are cached up to a maximum of 100 entries. If traceroute cache is disabled, traceroute replies are not cached; the default size is 0.

## Command Modes

Global configuration (config)

## Command History

| Release      | Modification                                                     |
|--------------|------------------------------------------------------------------|
| 12.2(33)SRA  | This command was introduced.                                     |
| 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T.    |
| 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.  |
| 12.2(33)SX12 | This command was integrated into Cisco IOS Release 12.2(33)SX12. |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.  |

## Usage Guidelines

Before you can issue this command, you must have enabled traceroute caching using the **ethernet cfm traceroute cache** command.

Entries in the traceroute cache table are single replies from remote devices—not the number of operations on the device. In Cisco pre-Standard CFM Draft 1 when the maximum cache size is reached, new replies cannot be added until you clear the cache or increase its size. In CFM IEEE 802.1ag Standard when the maximum cache size is reached, the oldest traceroute operation is removed to make room for a new traceroute operation.

Output of the **show running all** command displays “ethernet cfm traceroute cache size 100” when traceroute cache is enabled and the default value of 100 is configured.

Setting the number of entries lower than the number of entries currently cached causes this command to be rejected, and you are prompted to clear the traceroute cache.

## Examples

The following example shows how to set the maximum number of entries in an Ethernet CFM traceroute cache table to 2500:

```
Router(config)# ethernet cfm traceroute cache size 2500
```

| Related Commands | Command                                        | Description                                                                    |
|------------------|------------------------------------------------|--------------------------------------------------------------------------------|
|                  | <b>ethernet cfm traceroute cache</b>           | Enables caching of Ethernet CFM data learned from traceroute messages.         |
|                  | <b>ethernet cfm traceroute cache hold-time</b> | Sets the maximum time that Ethernet CFM traceroute cache entries are retained. |
|                  | <b>show running all</b>                        | Shows the running configuration with default values.                           |

# ethernet lmi

To set Ethernet local management interface (LMI) parameters for a user-network interface (UNI), use the **ethernet lmi** command in interface configuration mode. To remove Ethernet LMI parameters on a UNI, use the **no** form of this command.

**ethernet lmi** { **n391** | **n393** | **t391** | **t392** } *value*

**no ethernet lmi** { **n391** | **n393** | **t391** | **t392** }

| Syntax Description |             |                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>n391</b>        |             | Polling counter on the customer equipment. A polling counter polls the status of the UNI and all Ethernet virtual connections (EVCs).                                                                                                                                                                                                                                                                            |
| <b>n393</b>        |             | An error counter for customer equipment or for a metro Ethernet network.                                                                                                                                                                                                                                                                                                                                         |
| <b>t391</b>        |             | Polling timer on the customer equipment. A polling timer transmits status enquiries and when status messages are not received, records errors.                                                                                                                                                                                                                                                                   |
| <b>t392</b>        |             | Polling verification timer on the metro Ethernet network. The polling verification timer verifies status enquiries received. When a timer expires, an error is recorded and the timer is restarted.                                                                                                                                                                                                              |
|                    | <b>Note</b> | The t392 timer is valid only on Ethernet LMI provider edge (PE) devices. It is not available on customer edge (CE) devices.                                                                                                                                                                                                                                                                                      |
| <i>value</i>       |             | Integer value within ranges that vary depending on the keyword with which it is used. Valid values are as follows: <ul style="list-style-type: none"> <li><b>n391</b>—1 to 65000. Default is 360.</li> <li><b>n393</b>—1 to 10. Default is 4.</li> <li><b>t391</b>—5 to 30 (seconds). Default is 10.</li> <li><b>t392</b>—5 to 30 (seconds); default is 15 or 0 to 0 (0–0), which disables the timer.</li> </ul> |

**Command Default** Ethernet LMI parameters are not set on any UNIs.

**Command Modes** Interface configuration (config-if)

| Command History | Release     | Modification                                                                                         |
|-----------------|-------------|------------------------------------------------------------------------------------------------------|
|                 | 12.4(9)T    | This command was introduced.                                                                         |
|                 | 12.2(33)SRB | Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                      |

---

**Usage Guidelines**

The value for the polling verification timer (t392) should be greater than the value for the polling timer (t391).

The polling verification timer (t392) can be disabled.

A very high value for the polling timer (t391) means more time spent detecting Ethernet LMI link-down errors.

---

**Examples**

The following example shows how to set a polling counter for 30 seconds on interface Ethernet 1/0:

```
Router# configure terminal
Router(config)# interface ethernet 1/0
Router(config-if)# ethernet lmi t391 30
```

# ethernet lmi global

To enable Ethernet local management interface (LMI) functionality globally on a device, use the **ethernet lmi global** command in global configuration mode. To disable Ethernet LMI globally on a device, use the **no** form of this command.

**ethernet lmi global**

**no ethernet lmi global**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Ethernet LMI is disabled.

**Command Modes** Global configuration (config)

| Command History | Release     | Modification                                                                                         |
|-----------------|-------------|------------------------------------------------------------------------------------------------------|
|                 | 12.4(9)T    | This command was introduced.                                                                         |
|                 | 12.2(33)SRB | Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                      |

**Usage Guidelines** Ethernet LMI is disabled by default on an interface and must be explicitly enabled. The **ethernet lmi global** command enables Ethernet LMI on all interfaces for an entire device. The benefit of this command is that you can enable Ethernet LMI on all interfaces with one command compared to enabling Ethernet LMI separately on each interface.

To disable Ethernet LMI on a specific interface after the **ethernet lmi global** command has been issued, the **no ethernet lmi interface** command must be issued on that interface.

The sequence in which the **ethernet lmi interface** and **ethernet lmi global** commands are issued is significant. The latest command issued overrides the prior command issued.

**Examples** The following example shows how to enable Ethernet LMI globally on a device:

```
Router(config)# ethernet lmi global
```

| Related Commands | Command                       | Description                                        |
|------------------|-------------------------------|----------------------------------------------------|
|                  | <b>ethernet lmi interface</b> | Enables Ethernet LMI for a user-network interface. |

# ethernet lmi interface

To enable Ethernet local management interface (LMI) on a user-network interface (UNI), use the **ethernet lmi interface** command in interface configuration mode. To remove Ethernet LMI on a UNI, use the **no** form of this command.

**ethernet lmi interface**

**no ethernet lmi interface**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Ethernet LMI parameters are not set on any UNIs.

**Command Modes** Interface configuration (config-if)

## Command History

| Release     | Modification                                                                                         |
|-------------|------------------------------------------------------------------------------------------------------|
| 12.4(9)T    | This command was introduced.                                                                         |
| 12.2(33)SRB | Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                      |

## Usage Guidelines

This command enables Ethernet LMI processing on an interface if the **ethernet lmi global** command has not been issued. When the **ethernet lmi global** command has been issued, Ethernet LMI is enabled on all interfaces. In this case, the **no ethernet lmi interface** command overrides the **ethernet lmi global** command and disables Ethernet LMI processing on the interface.

The sequence in which the commands are issued is significant. The latest command issued overrides the prior command issued.

## Examples

The following example shows how to enable Ethernet LMI on interface Ethernet 1/0:

```
Router# configure terminal
Router(config)# interface ethernet 1/0
Router(config-if)# ethernet lmi interface
```

## Related Commands

| Command                    | Description                                              |
|----------------------------|----------------------------------------------------------|
| <b>ethernet lmi global</b> | Enables Ethernet LMI functionality globally on a device. |



# ethernet oam

To enable Ethernet operations, maintenance, and administration (OAM) on an interface, use the **ethernet oam** command in interface configuration mode. To disable Ethernet OAM on an interface, use the **no** form of this command.

**ethernet oam** [**max-rate** *oampdus* | **min-rate** *num-seconds* | **mode** {**active** | **passive**} | **timeout** *seconds*]

**no ethernet oam** [**max-rate** | **min-rate** | **mode** {**active** | **passive**} | **timeout**]

| Syntax Description |  |                                                                                                                                                     |
|--------------------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>max-rate</b>    |  | (Optional) Sets the maximum rate that OAM protocol data units (PDUs) can be sent per second.                                                        |
| <i>oampdus</i>     |  | (Optional) Integer in the range of 1 to 10 that is the number of OAM PDUs transmitted. The default is 10 for the maximum rate.                      |
| <b>min-rate</b>    |  | (Optional) Controls the minimum rate that OAM PDUs are transmitted, in seconds.                                                                     |
| <i>num-seconds</i> |  | (Optional) Integer in the range of 1 to 10 that is the number of seconds during which at least one OAM PDU must be sent.                            |
| <b>mode</b>        |  | (Optional) Sets the OAM client mode.                                                                                                                |
| <b>active</b>      |  | (Optional) Sets the OAM client mode to active after the interface was previously placed in passive mode. Active is the default.                     |
| <b>passive</b>     |  | (Optional) Sets the OAM client mode to passive. In passive mode, a device cannot initiate discovery, inquire about variables, or set loopback mode. |
| <b>timeout</b>     |  | (Optional) Specifies the amount of time, in seconds, after which a device declares its OAM peer to be nonoperational.                               |
| <i>seconds</i>     |  | (Optional) Integer in the range of 2 to 30 that is the number of seconds of the timeout period. The default is 5.                                   |

**Command Default** Ethernet OAM is disabled.

**Command Modes** Interface configuration (config-if)

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(33)SRA | This command was introduced.                                    |
|                 | 12.4(15)T   | This command was integrated into Cisco IOS Release 12.4(15)T.   |
|                 | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

---

**Usage Guidelines**

When Ethernet OAM is configured on an interface, the default mode of the OAM client is active. When the Ethernet OAM mode is enabled on two interfaces passing traffic, both interfaces cannot be in passive mode. Both interfaces can be in active mode, and one can be in active mode and the other in passive mode. You can toggle between Ethernet OAM modes without disabling OAM.

The **min-rate** *num-seconds* keyword and argument pair controls the minimum rate at which OAM PDUs can be sent on an interface, in seconds. A value of *n*, where 1 is less than or equal to *n* and *n* is less than or equal to 10, indicates that an OAM PDU must be sent at least once per *n* seconds. If no other OAM PDU is to be sent within an *n*-second window, an information OAM PDU must be sent.

---

**Examples**

The following example shows how to activate an Ethernet OAM interface that was previously configured to be in passive mode:

```
Router(config)# interface gigabitethernet 0/1
Router(config-if)# ethernet oam mode active
```

The following example shows how to set the maximum transmission rate of OAM PDUs on interface GigabitEthernet 0/1 to 5 transmissions per second:

```
Router(config)# interface gigabitethernet 0/1
Router(config-if)# ethernet oam max-rate 5
```

The following example shows how to set the timeout period to 25 seconds on interface GigabitEthernet 0/1:

```
Router(config)# interface gigabitethernet 0/1
Router(config-if)# ethernet oam timeout 25
```

# ethernet oam link-monitor frame

To configure an error frame threshold or window on an Ethernet operations, maintenance, and administration (OAM) interface, use the **ethernet oam link-monitor frame** command in configuration template mode or interface configuration mode. To remove the threshold or window, use the **no** form of this command.

**ethernet oam link-monitor frame** { **threshold** { **high** { **none** | *high-frames* } | **low** *low-frames* } | **window** *milliseconds* }

**no ethernet oam link-monitor frame** { **threshold** { **high** | **low** } | **window** }

| Syntax Description | threshold           | Sets a number of error frames at, above, or below which an action is triggered.                                      |
|--------------------|---------------------|----------------------------------------------------------------------------------------------------------------------|
|                    | high                | Sets a high error frame threshold in number of frames.                                                               |
|                    | none                | Disables a high threshold.                                                                                           |
|                    | <i>high-frames</i>  | Integer in the range of 1 to 65535 that is the high threshold in number of frames.                                   |
|                    | low                 | Sets a low error frame threshold.                                                                                    |
|                    | <i>low-frames</i>   | Integer in the range of 0 to 65535 that sets the low threshold in number of frames. The default is 1.                |
|                    | window              | Sets a window and period of time during which error frames are counted.                                              |
|                    | <i>milliseconds</i> | Integer in the range of 10 to 600 that represents a number of milliseconds in a multiple of 100. The default is 100. |

**Command Default** The **ethernet oam link-monitor frame** command is not configured.

**Command Modes** Configuration template (config-template)  
Interface configuration (config-if)

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(33)SRA | This command was introduced.                                    |
|                 | 12.4(15)T   | This command was integrated into Cisco IOS Release 12.4(15)T.   |
|                 | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** The **ethernet oam link-monitor frame** command configures a number of error frames that triggers an action or a period of time in which error frames are counted.

**Examples**

The following example shows how to configure an Ethernet OAM link-monitor frame window of 3000 milliseconds:

```
Router(config-template)# ethernet oam link-monitor frame window 300
```

**Related Commands**

|                                                        |                                                                                                                    |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>ethernet oam link-monitor frame-period</b>          | Configures an error frame period on an Ethernet OAM interface.                                                     |
| <b>ethernet oam link-monitor frame-seconds</b>         | Configures a frame-seconds period on an Ethernet OAM interface.                                                    |
| <b>ethernet oam link-monitor high-threshold action</b> | Configures a specific action to occur when a high threshold for an error is exceeded on an Ethernet OAM interface. |
| <b>ethernet oam link-monitor receive-crc</b>           | Configures an Ethernet OAM interface to monitor frames received with CRC errors for a period of time.              |
| <b>ethernet oam link-monitor symbol-period</b>         | Configures an error symbol period on an Ethernet OAM interface.                                                    |
| <b>ethernet oam link-monitor transmit-crc</b>          | Configures an Ethernet OAM interface to monitor frames transmitted with CRC errors for a period of time.           |

# ethernet oam link-monitor frame-period

To configure an error frame period on an Ethernet operations, maintenance, and administration (OAM) interface, use the **ethernet oam link-monitor frame-period** command in configuration template or interface configuration mode. To remove the frame period, use the **no** form of this command.

**ethernet oam link-monitor frame-period** { **threshold** { **high** { **none** | *high-frames* } | **low** *low-frames* } | **window** *frames* }

**no ethernet oam link-monitor frame-period** { **threshold** { **high** | **low** } | **window** }

| Syntax Description |  |                                                                                                                                                |
|--------------------|--|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>threshold</b>   |  | Sets a number of error frames for the period at, above, or below which an action is triggered.                                                 |
| <b>high</b>        |  | Sets a high threshold for the error frame period in number of frames.                                                                          |
| <b>none</b>        |  | Disables a high threshold.                                                                                                                     |
| <i>high-frames</i> |  | Integer in the range of 1 to 65535 that is the high threshold in number of frames. There is no default. The high threshold must be configured. |
| <b>low</b>         |  | Sets a low threshold for the error frame period in number of frames.                                                                           |
| <i>low-frames</i>  |  | Integer in the range of 0 to 65535 that is the low threshold in number of frames. The default is 1.                                            |
| <b>window</b>      |  | Sets a polling window and window size.                                                                                                         |
| <i>frames</i>      |  | Integer in the range of 1 to 65535 that is the window size in number of frames. Each value is a multiple of 10000. The default is 1000.        |

**Command Default** The **ethernet oam link-monitor frame-period** command is not configured.

**Command Modes** Configuration template (config-template)  
Interface configuration (config-if)

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(33)SRA | This command was introduced.                                    |
|                 | 12.4(15)T   | This command was integrated into Cisco IOS Release 12.4(15)T.   |
|                 | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** The **ethernet oam link-monitor frame-period** command configures an error frame period in number of frames. When a high threshold is configured, it must be at least as great as the low threshold for frame errors.

The number of frames polled is user defined. Note that the system can poll only by time, not by frames. The number of frames you specify is converted internally to seconds using a formula that includes interface speed.

**Examples**

The following example shows how to configure an Ethernet OAM link-monitor frame-period window of 20000 frames:

```
Router(config-template)# ethernet oam link-monitor frame-period window 2
```

The following example shows how to configure an Ethernet OAM link-monitor frame-period low threshold of 500 frames:

```
Router(config-template)# ethernet oam link-monitor frame-period threshold low 500
```

**Related Commands**

|                                                        |                                                                                                                    |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>ethernet oam link-monitor frame</b>                 | Configures an error frame threshold or window on an Ethernet OAM interface.                                        |
| <b>ethernet oam link-monitor frame-seconds</b>         | Configures a frame-seconds period on an Ethernet OAM interface.                                                    |
| <b>ethernet oam link-monitor high-threshold action</b> | Configures a specific action to occur when a high threshold for an error is exceeded on an Ethernet OAM interface. |
| <b>ethernet oam link-monitor receive-crc</b>           | Configures an Ethernet OAM interface to monitor frames received with CRC errors for a period of time.              |
| <b>ethernet oam link-monitor symbol-period</b>         | Configures an error symbol period on an Ethernet OAM interface.                                                    |
| <b>ethernet oam link-monitor transmit-crc</b>          | Configures an Ethernet OAM interface to monitor frames transmitted with CRC errors for a period of time.           |

# ethernet oam link-monitor frame-seconds

To configure a frame-seconds period on an Ethernet operations, maintenance, and administration (OAM) interface, use the **ethernet oam link-monitor frame-seconds** command in configuration template and interface configuration mode. To remove the threshold or window, use the **no** form of this command.

```
ethernet oam link-monitor frame-seconds { threshold { high { none | high-frames } | low  
low-frames } | window milliseconds }
```

```
no ethernet oam link-monitor frame-seconds { threshold { high | low } | window }
```

| Syntax Description | threshold    | Sets a number at, above, or below which an action is triggered.                                                                              |
|--------------------|--------------|----------------------------------------------------------------------------------------------------------------------------------------------|
|                    | high         | Sets a high error frame-seconds threshold in number of seconds.                                                                              |
|                    | none         | Disables a high threshold.                                                                                                                   |
|                    | high-frames  | Integer in the range of 1 to 900 that is the high threshold in number of frames. There is no default. The high threshold must be configured. |
|                    | low          | Sets a low error frame-seconds threshold in number of seconds.                                                                               |
|                    | low-frames   | Integer in the range of 1 to 900 that sets the low threshold in number of frames. The default is 1.                                          |
|                    | window       | Sets a polling window during which error frames are counted.                                                                                 |
|                    | milliseconds | Integer in the range of 100 to 9000 that represents a number of milliseconds in a multiple of 100. The default is 1000.                      |

|                 |                                                                               |
|-----------------|-------------------------------------------------------------------------------|
| Command Default | The <b>ethernet oam link-monitor frame-seconds</b> command is not configured. |
|-----------------|-------------------------------------------------------------------------------|

|               |                                                                                 |
|---------------|---------------------------------------------------------------------------------|
| Command Modes | Configuration template (config-template)<br>Interface configuration (config-if) |
|---------------|---------------------------------------------------------------------------------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(33)SRA | This command was introduced.                                    |
|                 | 12.4(15)T   | This command was integrated into Cisco IOS Release 12.4(15)T.   |
|                 | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                  |                                                                                                                                                                               |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usage Guidelines | The <b>ethernet oam link-monitor frame-seconds</b> command configures a number of error frames that triggers an action or a period of time in which error frames are counted. |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Examples

The following example shows how to configure an Ethernet OAM link-monitor frame-seconds window of 30000 milliseconds (30 seconds):

```
Router(config-template)# ethernet oam link-monitor frame-seconds window 300
```

Related Commands

|                                                 |                                                                                                                    |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| ethernet oam link-monitor frame                 | Configures an error frame threshold or window on an Ethernet OAM interface.                                        |
| ethernet oam link-monitor frame-period          | Configures an error frame period on an Ethernet OAM interface.                                                     |
| ethernet oam link-monitor high-threshold action | Configures a specific action to occur when a high threshold for an error is exceeded on an Ethernet OAM interface. |
| ethernet oam link-monitor receive-crc           | Configures an Ethernet OAM interface to monitor frames received with CRC errors for a period of time.              |
| ethernet oam link-monitor symbol-period         | Configures an error symbol period on an Ethernet OAM interface.                                                    |
| ethernet oam link-monitor transmit-crc          | Configures an Ethernet OAM interface to monitor frames transmitted with CRC errors for a period of time.           |



# ethernet oam link-monitor high-threshold action

To configure a specific action to occur when a high threshold for an error is exceeded on an Ethernet operations, maintenance, and administration (OAM) interface, use the **ethernet oam link-monitor high-threshold action** command in configuration template mode. To remove the high-threshold action, use the **no** form of this command.

**ethernet oam link-monitor high-threshold action {error-disable-interface | failover}**

**no ethernet oam link-monitor high-threshold action**

## Syntax Description

|                                |                                                              |
|--------------------------------|--------------------------------------------------------------|
| <b>error-disable-interface</b> | Performs an error-disable function on the interface.         |
| <b>failover</b>                | Performs a failover to another port in the same PortChannel. |

## Command Default

A high-threshold action is not configured.

## Command Modes

Configuration template (config-template)

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(33)SRA | This command was introduced.                                    |
| 12.4(15)T   | This command was integrated into Cisco IOS Release 12.4(15)T.   |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

The failover action is applicable only to EtherChannel interfaces. It provides an automatic failover of traffic from one port in an EtherChannel to another port in the same EtherChannel when one of the ports in the channel exceeds the high threshold for an error within the specified interval. The port failover occurs only if at least one operational port is in the EtherChannel. The failed port is put into an error-disable state. If the failed port is the last port in the EtherChannel, the port is not put into the error-disable state and continues to pass traffic regardless of the types of errors received.

Single, nonchanneling ports go into the error-disable state when the error high threshold is exceeded within the specified interval.

## Examples

The following example shows how to configure an error-disable-interface action to occur when the high threshold for an error is exceeded:

```
Router(config-template)# ethernet oam link-monitor high-threshold action  
error-disable-interface
```

|                         |                                                |                                                                                                          |
|-------------------------|------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>Related Commands</b> | <b>ethernet oam link-monitor frame</b>         | Configures an error frame threshold or window on an Ethernet OAM interface.                              |
|                         | <b>ethernet oam link-monitor frame-period</b>  | Configures an error frame period on an Ethernet OAM interface.                                           |
|                         | <b>ethernet oam link-monitor frame-seconds</b> | Configures a frame-seconds period on an Ethernet OAM interface.                                          |
|                         | <b>ethernet oam link-monitor receive-crc</b>   | Configures an Ethernet OAM interface to monitor frames received with CRC errors for a period of time.    |
|                         | <b>ethernet oam link-monitor symbol-period</b> | Configures an error symbol period on an Ethernet OAM interface.                                          |
|                         | <b>ethernet oam link-monitor transmit-crc</b>  | Configures an Ethernet OAM interface to monitor frames transmitted with CRC errors for a period of time. |

# ethernet oam link-monitor on

To enable link monitoring on an Ethernet operations, maintenance, and administration (OAM) interface, use the **ethernet oam link-monitor on** command in interface configuration mode. To disable link monitoring, use the **no** form of this command.

**ethernet oam link-monitor on**

**no ethernet oam link-monitor on**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Link monitoring is turned on when Ethernet OAM is enabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(33)SRA | This command was introduced.                                    |
| 12.4(15)T   | This command was integrated into Cisco IOS Release 12.4(15)T.   |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

When link monitoring is enabled, the interface sends event OAM protocol data units (PDUs) when errors occur and interprets event OAM PDUs from the remote peer. Link monitoring can be effective only if both the local client and remote peer agree to support it.

The **ethernet oam link-monitor on** command is enabled by default when Ethernet OAM is enabled and does not display in the configuration when the **show running-config** command is issued.

When link monitoring is enabled by default, to turn it off you must explicitly disable it by issuing the **no** form of this command.

## Examples

The following example shows how to disable link monitoring on Ethernet OAM interface Ethernet 0/1:

```
Router(config)# interface ethernet 0/1
Router(config-if)# no ethernet oam link-monitor on
```

## Related Commands

|                                            |                                                                   |
|--------------------------------------------|-------------------------------------------------------------------|
| <b>ethernet oam link-monitor supported</b> | Enables support for link monitoring on an Ethernet OAM interface. |
|--------------------------------------------|-------------------------------------------------------------------|

# ethernet oam link-monitor receive-crc

To configure an Ethernet operations, maintenance, and administration (OAM) interface to monitor ingress frames received with cyclic redundancy code (CRC) errors for a period of time, use the **ethernet oam link-monitor receive-crc** command in configuration template or interface configuration mode. To disable monitoring, use the **no** form of this command.

```
ethernet oam link-monitor receive-crc { threshold { high { high-frames | none } | low low-frames }
| window milliseconds }
```

```
no ethernet oam link-monitor receive-crc { threshold { high | low } | window }
```

## Syntax Description

|                     |                                                                                                                        |
|---------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>threshold</b>    | Sets a number of frames with CRC errors received at, above, or below which an action is triggered.                     |
| <b>high</b>         | Sets a high threshold in number of frames.                                                                             |
| <i>high-frames</i>  | Integer in the range of 1 to 65535 that is the high threshold in number of frames.                                     |
| <b>none</b>         | Disables a high threshold.                                                                                             |
| <b>low</b>          | Sets a low threshold.                                                                                                  |
| <i>low-frames</i>   | Integer in the range of 0 to 65535 that sets the low threshold in number of frames. The default is 10.                 |
| <b>window</b>       | Sets a window and period of time during which frames with CRC errors are counted.                                      |
| <i>milliseconds</i> | Integer in the range of 10 to 1800 that represents a number of milliseconds in a multiple of 100. The default is 1000. |

## Command Default

The **ethernet oam link-monitor receive-crc** command is not configured.

## Command Modes

Configuration template (config-template)  
Interface configuration (config-if)

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(33)SRA | This command was introduced.                                    |
| 12.4(15)T   | This command was integrated into Cisco IOS Release 12.4(15)T.   |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

OAM must be operational on the interface before you issue this command.

**Examples**

The following example shows how to configure a receive-crc period with a low threshold of 3000:

```
Router(config-if)# ethernet oam link-monitor receive-crc threshold low 3000
```

**Related Commands**

|                                                        |                                                                                                                    |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>ethernet oam link-monitor frame</b>                 | Configures an error frame threshold or window on an Ethernet OAM interface.                                        |
| <b>ethernet oam link-monitor frame-period</b>          | Configures an error frame period on an Ethernet OAM interface.                                                     |
| <b>ethernet oam link-monitor frame-seconds</b>         | Configures a frame-seconds period on an Ethernet OAM interface.                                                    |
| <b>ethernet oam link-monitor high-threshold action</b> | Configures a specific action to occur when a high threshold for an error is exceeded on an Ethernet OAM interface. |
| <b>ethernet oam link-monitor symbol-period</b>         | Configures an error symbol period on an Ethernet OAM interface.                                                    |
| <b>ethernet oam link-monitor transmit-crc</b>          | Configures an Ethernet OAM interface to monitor frames transmitted with CRC errors for a period of time.           |

# ethernet oam link-monitor supported

To enable support for link monitoring on an Ethernet operations, maintenance, and administration (OAM) interface, use the **ethernet oam link-monitor supported** command in interface configuration mode. To disable link monitoring support, use the **no** form of this command.

**ethernet oam link-monitor supported**

**no ethernet oam link-monitor supported**

Syntax Description

This command has no arguments or keywords.

Command Default

Link monitoring is supported when Ethernet OAM is enabled.

Command Modes

Interface configuration (config-if)

Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(33)SRA | This command was introduced.                                    |
| 12.4(15)T   | This command was integrated into Cisco IOS Release 12.4(15)T.   |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

Usage Guidelines

Use this command to help establish an OAM session for performing OAM functions, such as remote loopback. For example, if your device is connected to a third-party device that does not support link monitoring, you must disable link monitoring support on your device to establish an OAM session with the third-party device.

When the **ethernet oam link-monitor supported** command has been issued, remote loopback does not function, whether or not an interface has been configured to support it.

The **ethernet oam link-monitor supported** command is enabled by default when Ethernet OAM is enabled and does not display in the configuration when the **show running-config** command is issued.

When support for link monitoring is enabled by default, to turn it off you must explicitly disable it by issuing the **no** form of this command.

Examples

The following example shows how to disable support for link monitoring on the GigabitEthernet 0/1 OAM interface:

```
Router(config)# interface gigabitethernet 0/1
Router(config-if)# no ethernet oam link-monitor supported
```

The following example shows how to reenable support for link monitoring on the GigabitEthernet 0/1 OAM interface after support has been disabled:

```
Router(config)# interface gigabitethernet 0/1
Router(config-if)# ethernet oam link-monitor supported
```

#### Related Commands

|                                     |                                                       |
|-------------------------------------|-------------------------------------------------------|
| <b>ethernet oam link-monitor on</b> | Enables link monitoring on an Ethernet OAM interface. |
|-------------------------------------|-------------------------------------------------------|

# ethernet oam link-monitor transmit-crc

To configure an Ethernet operations, maintenance, and administration (OAM) interface to monitor egress frames transmitted with cyclic redundancy code (CRC) errors for a period of time, use the **ethernet oam link-monitor transmit-crc** command in configuration template or interface configuration mode. To disable monitoring, use the **no** form of this command.

**ethernet oam link-monitor transmit-crc** { **threshold** { **high** { *high-frames* | **none** } | **low** *low-frames* } | **window** *milliseconds* }

**no ethernet oam link-monitor transmit-crc** { **threshold** { **high** | **low** } | **window** }

## Syntax Description

|                     |                                                                                                                       |
|---------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>threshold</b>    | Sets a number of frames with CRC errors transmitted at, above, or below which an action is triggered.                 |
| <b>high</b>         | Sets a high threshold in number of frames.                                                                            |
| <i>high-frames</i>  | Integer in the range of 1 to 65535 that is the high threshold in number of frames.                                    |
| <b>none</b>         | Disables a high threshold.                                                                                            |
| <b>low</b>          | Sets a low threshold.                                                                                                 |
| <i>low-frames</i>   | Integer in the range of 0 to 65535 that sets the low threshold in number of frames. The default is 10.                |
| <b>window</b>       | Sets a window and period of time during which frames with transmit CRC errors are counted.                            |
| <i>milliseconds</i> | Integer in the range of 10 to 1800 that represents a number of milliseconds in a multiple of 100. The default is 100. |

## Command Default

The **ethernet oam link-monitor transmit-crc** command is not configured.

## Command Modes

Configuration template (config-template)  
Interface configuration (config-if)

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(33)SRA | This command was introduced.                                    |
| 12.4(15)T   | This command was integrated into Cisco IOS Release 12.4(15)T.   |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

OAM must be operational on the interface before you issue this command.



---

**Examples**

The following example shows how to configure a transmit CRC window of 2500 milliseconds:

```
Router(config-if)# ethernet oam link-monitor transmit-crc window 25
```

---

**Related Commands**

|                                                        |                                                                                                                    |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>ethernet oam link-monitor frame</b>                 | Configures an error frame threshold or window on an Ethernet OAM interface.                                        |
| <b>ethernet oam link-monitor frame-period</b>          | Configures an error frame period on an Ethernet OAM interface.                                                     |
| <b>ethernet oam link-monitor frame-seconds</b>         | Configures a frame-seconds period on an Ethernet OAM interface.                                                    |
| <b>ethernet oam link-monitor high-threshold action</b> | Configures a specific action to occur when a high threshold for an error is exceeded on an Ethernet OAM interface. |
| <b>ethernet oam link-monitor receive-crc</b>           | Configures an Ethernet OAM interface to monitor frames received with CRC errors for a period of time.              |
| <b>ethernet oam link-monitor symbol-period</b>         | Configures an error symbol period on an Ethernet OAM interface.                                                    |

# ethernet oam mib log size

To set the size of the Ethernet Operations, Administration, and Maintenance (OAM) event log table, use the **ethernet oam mib log size** command in global configuration mode. To remove the event log table, use the **no** form of this command.

**ethernet oam mib log size** *entries*

**no ethernet oam mib log size**

|                    |                |                                                                                                                                       |
|--------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>entries</i> | Number of entries that the event log table holds. Integer from 0 to 200. The minimum is 0, the maximum is 200, and the default is 50. |
|--------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                       |
|-----------------|---------------------------------------|
| Command Default | An event log table is not configured. |
|-----------------|---------------------------------------|

|               |                               |
|---------------|-------------------------------|
| Command Modes | Global configuration (config) |
|---------------|-------------------------------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(33)SRD | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                  |                                                       |
|------------------|-------------------------------------------------------|
| Usage Guidelines | Use this command to configure an OAM event log table. |
|------------------|-------------------------------------------------------|

|          |                                                                                       |
|----------|---------------------------------------------------------------------------------------|
| Examples | The following example shows how to set the size of an event log table to 100 entries: |
|----------|---------------------------------------------------------------------------------------|

```
Router# configure terminal
Router(config)# ethernet oam mib log size 100
```

# ethernet oam remote-failure action

To enable Ethernet Operations, Administration, and Maintenance (OAM) remote failure actions, use the **ethernet oam remote-failure action** command in interface configuration mode. To turn off remote failure actions, use the **no** form of this command.

```
ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action
                             {error-block-interface | error-disable-interface}
```

```
no ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action
```

| Syntax Description |                                |                                                                |
|--------------------|--------------------------------|----------------------------------------------------------------|
|                    | <b>critical-event</b>          | Specifies remote critical event failures.                      |
|                    | <b>dying-gasp</b>              | Specifies remote dying-gasp failures.                          |
|                    | <b>link-fault</b>              | Specifies remote link-fault failures.                          |
|                    | <b>error-block-interface</b>   | Sets the interface to the blocking state when an error occurs. |
|                    | <b>error-disable-interface</b> | Disables the interface when an error occurs.                   |

|                        |                                                                   |
|------------------------|-------------------------------------------------------------------|
| <b>Command Default</b> | Actions in response to Ethernet OAM remote failures do not occur. |
|------------------------|-------------------------------------------------------------------|

|                      |                                     |
|----------------------|-------------------------------------|
| <b>Command Modes</b> | Interface configuration (config-if) |
|----------------------|-------------------------------------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(33)SRA | This command was introduced.                                    |
|                 | 12.2(33)SX1 | The <b>error-block-interface</b> keyword was added.             |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                                                                                                    |
|-------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | Use this command to configure an interface to take specific actions when Ethernet OAM remote-failure events occur. |
|-------------------------|--------------------------------------------------------------------------------------------------------------------|

Release 12.2(33)MRA does not support sending critical-event messages but can receive all three message types.

|                 |                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | The following example shows how to configure the action that the Ethernet 1/1 interface takes when a critical event occurs: |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------|

```
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet oam remote-failure critical-event action
error-disable-interface
```

# ethernet oam remote-loopback

To turn on or off Ethernet operations, maintenance, and administration (OAM) remote loopback functionality on an interface, use the **ethernet oam remote-loopback** command in privileged EXEC mode. This command does not have a no form.

**ethernet oam remote-loopback** {start | stop} {interface *type number*}

## Syntax Description

|                  |                                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------|
| <b>start</b>     | Starts the remote loopback operation.                                                            |
| <b>stop</b>      | Stops the remote loopback operation.                                                             |
| <b>interface</b> | Specifies an interface.                                                                          |
| <i>type</i>      | Type of Ethernet interface. Valid values are: FastEthernet, GigabitEthernet, TenGigabitEthernet. |
| <i>number</i>    | Integer from 1 to 9 that is the number of the Ethernet interface.                                |

## Command Default

Remote loopback functionality is turned off.

## Command Modes

Privileged EXEC (#)

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(33)SRA | This command was introduced.                                    |
| 12.4(15)T   | This command was integrated into Cisco IOS Release 12.4(15)T.   |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

There is no **no** form of this command.

When Ethernet OAM remote loopback functionality is enabled on an interface, traffic sent out on this interface is discarded or sent back (and dropped locally) by the remote interface.

Remote loopback does not function, whether or not an interface has been configured to support it, when the **no ethernet oam link-monitor supported** command has been issued.



### Note

To start Ethernet OAM remote loopback on a switch port, you must first configure the **access-group mode prefer port** command in interface configuration mode.

## Examples

The following example shows how to start a remote loopback session on interface GigabitEthernet 2/1:

```
Router# ethernet oam remote-loopback start interface gigabitethernet2/1
```

**Related Commands**

|                                                 |                                                                                                                                                        |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>access-group mode prefer port</b>            | Specifies the override modes and the non-override modes for an access group and specifies that the PACL mode takes precedence if PACLs are configured. |
| <b>ethernet oam remote-loopback (interface)</b> | Enables the support of Ethernet OAM remote loopback operation on an interface or sets a remote loopback timeout period.                                |

# ethernet oam remote-loopback (interface)

To enable the support of Ethernet operations, maintenance, and administration (OAM) remote loopback operations on an interface or set a remote loopback timeout period, use the **ethernet oam remote-loopback (interface)** command in interface configuration mode. To disable support or remove the timeout setting, use the **no** form of this command.

```
ethernet oam remote-loopback {supported | timeout seconds}

no ethernet oam remote-loopback {supported | timeout}
```

## Syntax Description

|                  |                                                                        |
|------------------|------------------------------------------------------------------------|
| <b>supported</b> | Supports the remote loopback functionality.                            |
| <b>timeout</b>   | Sets a master loopback timeout setting.                                |
| <i>seconds</i>   | Integer from 1 to 10 that is the number seconds of the timeout period. |

## Command Default

Remote loopback is not supported.

## Command Modes

Interface configuration (config-if)

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(33)SRA | This command was introduced.                                    |
| 12.4(15)T   | This command was integrated into Cisco IOS Release 12.4(15)T.   |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

This command enables the support of OAM remote-loopback on an interface. Only after this functionality is enabled can the local OAM client initiate the OAM remote loopback operation. Changing this setting causes the local OAM client to exchange configuration information with its remote peer.

The **no** form of the command is rejected if the interface is in the loopback mode.



### Note

To start Ethernet OAM remote loopback on a switch port, you must first configure the **access-group mode prefer port** command in interface configuration mode.

## Examples

The following example shows how to enable remote loopback support on interface GigabitEthernet 2/1:

```
Router(config)# interface gigabitethernet 2/1
Router(config-if)# ethernet oam remote-loopback supported
```

**Related Commands**

|                                      |                                                                                                                                                     |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>access-group mode prefer port</b> | Specifies the override modes and the nonoverride modes for an access group and specifies that the ACL mode takes precedence if ACLs are configured. |
| <b>ethernet oam remote-loopback</b>  | Turns on or off the remote loopback functionality.                                                                                                  |

## fair-queue (class-default)

To specify the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy, use the **fair-queue** command in policy-map class configuration mode. To delete the configured number of dynamic queues from the class-default policy, use the **no** form of this command.

**fair-queue** [*number-of-dynamic-queues*]

**no fair-queue** [*number-of-dynamic-queues*]

### Syntax Description

*number-of-dynamic-queues* (Optional) A power of 2 that specifies the number of dynamic queues. Range is from 16 to 4096.

### Command Default

The number of dynamic queues is derived from the interface or ATM permanent virtual circuit (PVC) bandwidth. See [Table 3](#) in the “Usage Guidelines” section for the default number of dynamic queues that weighted fair queueing (WFQ) and class-based WFQ (CBWFQ) use when they are enabled on an interface. See [Table 4](#) in the “Usage Guidelines” section for the default number of dynamic queues used when WFQ or CBWFQ is enabled on an ATM PVC.

### Command Modes

Policy-map class configuration

### Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(5)T    | This command was introduced.                                                                                                                                                      |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

### Usage Guidelines

This command can be used for the default class (commonly known as the class-default class) only. You can use it in conjunction with either the **queue-limit** command or the **random-detect** command.

The class-default class is the default class to which traffic is directed if that traffic does not satisfy the match criteria of other classes whose policy is defined in the policy map.

[Table 3](#) lists the default number of dynamic queues that class-based WFQ (CBWFQ) uses when it is enabled on an interface.



**Table 3** Default Number of Dynamic Queues as a Function of Interface Bandwidth

| Bandwidth Range                                       | Number of Dynamic Queues |
|-------------------------------------------------------|--------------------------|
| Less than or equal to 64 kbps                         | 16                       |
| More than 64 kbps and less than or equal to 128 kbps  | 32                       |
| More than 128 kbps and less than or equal to 256 kbps | 64                       |
| More than 256 kbps and less than or equal to 512 kbps | 128                      |
| More than 512 kbps                                    | 256                      |

Table 4 lists the default number of dynamic queues used when CBWFQ is enabled on an ATM PVC.

**Table 4** Default Number of Dynamic Queues as a Function of ATM PVC Bandwidth

| Bandwidth Range                                         | Number of Dynamic Queues |
|---------------------------------------------------------|--------------------------|
| Less than or equal to 128 kbps                          | 16                       |
| More than 128 kbps and less than or equal to 512 kbps   | 32                       |
| More than 512 kbps and less than or equal to 2000 kbps  | 64                       |
| More than 2000 kbps and less than or equal to 8000 kbps | 128                      |
| More than 8000 kbps                                     | 256                      |

## Examples

The following example configures policy for the default class included in the policy map called policy9. Packets that do not satisfy match criteria specified for other classes whose policies are configured in the same service policy are directed to the default class, for which 16 dynamic queues have been reserved. Because the **queue-limit** command is configured, tail drop is used for each dynamic queue when the maximum number of packets are enqueued and additional packets arrive.

```
policy-map policy9
  class class-default
    fair-queue 16
    queue-limit 20
```

The following example configures policy for the default class included in the policy map called policy8. The **fair-queue** command reserves 20 dynamic queues to be used for the default class. For congestion avoidance, Weighted Random Early Detection (WRED) packet drop is used, not tail drop.

```
policy-map policy8
  class class-default
    fair-queue 64
    random-detect
```

## Related Commands

| Command                          | Description                                                                                                           |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>queue-limit</b>               | Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map. |
| <b>random-detect (interface)</b> | Enables WRED or DWRED.                                                                                                |

# fair-queue (policy-map class)

To specify the number of queues to be reserved for use by a traffic class, use the **fair-queue** command in policy-map class configuration mode. To delete the configured number of queues from the traffic class, use the **no** form of this command.

**fair-queue** [*dynamic-queues*]

**no fair-queue** [*dynamic-queues*]

## Syntax Description

*dynamic-queues* (Optional) A number specifying the number of dynamic conversation queues. The number can be in the range of 16 to 4096.

## Command Default

No queues are reserved.

## Command Modes

Policy-map class configuration

## Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(5)T    | This command was introduced.                                                                                                                                                      |
| 12.0(5)XE   | This command was integrated into Cisco IOS Release 12.0(5)XE and implemented on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers.                            |
| 12.1(5)T    | This command was integrated into Cisco IOS Release 12.1(5)T and was implemented on VIP-enabled Cisco 7500 series routers.                                                         |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

## Usage Guidelines

On a VIP, the **fair-queue** command can be used for any traffic class (as opposed to non-VIP platforms, which can only use the **fair-queue** command in the default traffic class). The **fair-queue** command can be used in conjunction with either the **queue-limit** command or the **random-detect exponential-weighting-constant** command.

## Examples

The following example configures the default traffic class for the policy map called policy9 to reserve ten queues for packets that do not satisfy match criteria specified for other traffic classes whose policy is configured in the same service policy. Because the **queue-limit** command is configured, tail drop is used for each queue when the maximum number of packets is enqueued and additional packets arrive.

```
policy-map policy9
class class-default
fair-queue 10
queue-limit 20
```

The following example configures a service policy called policy8 that is associated with a user-defined traffic class called class1. The **fair-queue** command reserves 20 queues to be used for the service policy. For congestion avoidance, Weighted Random Early Detection (WRED) or distributed WRED (DWRED) packet drop is used, not tail drop.

```
policy-map policy8
class class1
fair-queue 20
random-detect exponential-weighting-constant 14
```

**Related Commands**

| Command                                                       | Description                                                                                                           |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>class class-default</b>                                    | Specifies the default traffic class for a service policy map.                                                         |
| <b>queue-limit</b>                                            | Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map. |
| <b>random-detect</b><br><b>exponential-weighting-constant</b> | Configures the WRED and DWRED exponential weight factor for the average queue size calculation.                       |

# idle-pattern

To specify the data pattern transmitted on the T1/E1 line when missing packets are detected on the PWE3 circuit, use the **idle-pattern** command in CEM configuration mode. To stop sending idle pattern data, use the **no** form of this command.

**idle-pattern** [*pattern*]

**no idle-pattern**

## Syntax Description

|                |                                                                                                                                |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|
| <i>pattern</i> | (Optional) An 8-bit hexadecimal number that is transmitted as the idle pattern. T1 and E1 channels require only this argument. |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|

## Command Default

For T1 or E1 channels, the default idle pattern is 0xFF.

## Command Modes

CEM circuit configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.3(7)T    | This command was introduced.                                    |
| 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

The idle-pattern data is sent to replace the data from missing packets.

## Examples

The following example shows how to specify a data pattern:

```
Router# config t
Router(config)# interface cem 0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# idle-pattern 0x55
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

## Related Commands

| Command    | Description                                  |
|------------|----------------------------------------------|
| <b>cem</b> | Enters circuit emulation configuration mode. |

| Command          | Description                                                                                                            |
|------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>cem class</b> | Applies the CEM interface parameters defined in the given CEM class name to the circuit.                               |
| <b>class cem</b> | Configures CEM interface parameters in a class that's applied to CEM interfaces together in global configuration mode. |

# ima-group

To define physical links as inverse multiplexing over ATM (IMA) group members, use the **ima-group** command in interface configuration mode. When you first perform the configuration or when you change the group number, the interface is automatically disabled, moved to the new group, and then enabled. To remove the group, use the **no** form of this command.

**ima-group** *group-number*

**no ima-group** *group-number*

## Syntax Description

|                     |                                                                                                                                                                     |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>group-number</i> | Specifies an IMA group number from 0 to 3. IMA groups can span multiple ports on a port adapter or shared port adapter (SPA) but cannot span port adapters or SPAs. |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Command Default

No IMA groups are defined.

## Command Modes

Interface configuration

## Command History

| Release      | Modification                                                                                                                                                                      |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(5)XK    | This command was introduced on Cisco 2600 and 3600 series routers.                                                                                                                |
| 12.0(5)T     | This command was integrated into Cisco IOS Release 12.0(5)T.                                                                                                                      |
| 12.0(5)XE    | Support for Cisco 7200 and 7500 series routers was added.                                                                                                                         |
| 12.0(7)XE1   | Support for Cisco 7100 series routers was added.                                                                                                                                  |
| 12.1(5)T     | Support for Cisco 7100, 7200, and 7500 series routers was added.                                                                                                                  |
| 12.2(33)SRA  | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.4 (11)XJ  | This command was integrated into Cisco IOS Release 12.4 (11)XJ.                                                                                                                   |
| 12.2SX       | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SRB2 | Support for Cisco 7600 series routers was added.                                                                                                                                  |
| 12.4(19)MR2  | This command was integrated into Cisco IOS Release 12.4(19)MR2.                                                                                                                   |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

## Usage Guidelines

Use the **ima-group** interface command to configure a T1/E1 IMA port adapter interface as part of an IMA group.

## Examples

The following example shows how to define an IMA group:

```
Router(config)# interface ATM0/0
Router(config-if)# no ip address
```

```
Router(config-if)# no atm ilmi-keepalive
Router(config-if)# ima-group 0
```

**Related Commands**

| Command                       | Description                                                                   |
|-------------------------------|-------------------------------------------------------------------------------|
| <b>interface atm</b>          | Configures an ATM interface.                                                  |
| <b>interface atm ima</b>      | Configures an ATM IMA group.                                                  |
| <b>show ima interface atm</b> | Provides information about all configured IMA groups or a specific IMA group. |

# interface atm ima

To configure an ATM IMA group and enter interface configuration mode, use the **interface atm ima** global configuration command. If the group does not exist when the command is issued, the command automatically creates the group.

**interface atm** *slot/imagroup-number*

|                           |                     |                                                                              |
|---------------------------|---------------------|------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>slot</i>         | Specifies the slot location of the ATM IMA port adapter.                     |
|                           | <i>group-number</i> | Specifies an IMA group number from 0 to 3. You can create up to four groups. |

**Command Default** The interface includes individual ATM links, but no IMA groups.

**Command Modes** Global configuration

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                                                               |
|------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        |                |                                                                                                                                                                                   |
|                        | 12.0(5)XK      | This command was introduced on Cisco 2600 and 3600 series routers.                                                                                                                |
|                        | 12.0(5)T       | This command was integrated into Cisco IOS 12.0(5)T.                                                                                                                              |
|                        | 12.0(5)XE      | Support for Cisco 7200 and 7500 series routers was added.                                                                                                                         |
|                        | 12.0(7)XE1     | Support for Cisco 7100 series routers was added.                                                                                                                                  |
|                        | 12.1(5)T       | Support for Cisco 7100, 7200, and 7500 series routers was integrated into Cisco IOS Release 12.1(5)T.                                                                             |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                        | 12.2SX         | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                        | 12.4(19)MR2    | This command was incorporated into Cisco IOS Release 12.4(19)MR2.                                                                                                                 |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

**Usage Guidelines** When a port is configured for IMA functionality, it no longer operates as an individual ATM link. Specifying ATM links as members of a group using the **ima-group** interface command does not enable the group. You must use the **interface atm slot/imagroup-number** command to create the group.

**Examples** The following example shows the how to create the IMA group:

```
Router(config)# interface ATM0/IMA0
Router(config-if)# no ip address
```



| Related Commands | Command                       | Description                                                                                                                                               |
|------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>ima-group</b>              | Configures the physical links as IMA group members; execute this interface configuration command for each physical link that you include in an IMA group. |
|                  | <b>ima group-id</b>           | Enables the user to configure the IMA Group ID for the IMA interface.                                                                                     |
|                  | <b>interface atm</b>          | Configures physical links for an ATM interface.                                                                                                           |
|                  | <b>show ima interface atm</b> | Displays general and detailed information about IMA groups and the links they include.                                                                    |

# ip igmp join-group

To configure an interface on the router to join the specified group or channel, use the **ip igmp join-group** command in interface configuration mode. To cancel membership in a multicast group, use the **no** form of this command.

```
ip igmp join-group group-address
no ip igmp join-group group-address
```

|                    |               |                          |
|--------------------|---------------|--------------------------|
| Syntax Description | group-address | Multicast group address. |
|--------------------|---------------|--------------------------|

|                 |                                                |
|-----------------|------------------------------------------------|
| Command Default | No multicast group memberships are predefined. |
|-----------------|------------------------------------------------|

|               |                         |
|---------------|-------------------------|
| Command Modes | Interface configuration |
|---------------|-------------------------|

| Command History | Release     | Modification                                                                                                                                                                      |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 10.0        | This command was introduced.                                                                                                                                                      |
|                 | 12.3(14)T   | This command was modified. The <b>source</b> keyword and <i>source-address</i> argument were added.                                                                               |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                 | 12.2(33)SRE | This command was modified. The <b>source</b> keyword and <i>source-address</i> argument were added.                                                                               |
|                 | 12.2(33)MRB | This command was integrated into Cisco IOS Release 12.2(33)MRB. The <b>source</b> keyword is not supported in this release.                                                       |

|                  |                                                                                                                                                                                                                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usage Guidelines | Use the <b>ip igmp join-group</b> command to configure an interface on the router to join the specified group or channel. With this method, the router accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the router from fast switching. |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

  
Note

Multiple **ip igmp join-group** command configurations with different source addresses for the same group are supported.

## Examples

The following example shows how to configure a router to forward multicast traffic in the absence of directly connected IGMP hosts using the **ip igmp join-group** command. With this method, the router accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the router from fast switching. In this example, Fast Ethernet interface 0/0 on the router is configured to join the group 225.2.2.2.

```
interface FastEthernet0/0
 ip igmp join-group 225.2.2.2
```

## Related Commands

| Command                     | Description                                                 |
|-----------------------------|-------------------------------------------------------------|
| <b>ip igmp static-group</b> | Configures static group membership entries on an interface. |

# ip igmp query-interval



## Note

We recommend that you do not change the default IGMP query interval.

To configure the frequency at which the IGMP querier sends Internet Group Management Protocol (IGMP) host-query messages from an interface, use the **ip igmp query-interval** command in interface configuration mode. To restore the default IGMP query interval, use the **no** form of this command.

**ip igmp query-interval** *seconds*

**no ip igmp query-interval**

## Syntax Description

|                |                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <i>seconds</i> | Frequency, in seconds, at which the router sends IGMP query messages from the interface. The range is from 1 to 18000. The default is 60. |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------|

## Command Default

The default IGMP query interval is 60 seconds.

## Command Modes

Interface configuration (config-if)

## Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.2        | This command was introduced.                                                                                                                                                      |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)MRB | This command was integrated into Cisco IOS Release 12.2(33)MRB.                                                                                                                   |

## Usage Guidelines

Use the **ip igmp query-interval** command to configure the frequency at which the IGMP querier sends IGMP host-query messages from an interface. The IGMP querier sends query-host messages to discover which multicast groups have members on the attached networks of the router.



## Note

We recommend that you use the default IGMP query interval and timeout period.

The Cisco IOS software uses a default IGMP query interval of 60 seconds, which is different from the RFC standard default of 125 seconds. Using a lower default IGMP query interval of 60 seconds allows routers to stop forwarding traffic faster when a member crashes without sending leaves (in IGMPv2 or IGMPv3 environment), or if using IGMPv1: 3 \* 60 seconds versus 3 \* 125 seconds.

If a lower version IGMP-enabled interface (that is, an interface running IGMPv1 or v2) receives a higher version IGMP query (IGMPv3) with a different query interval, the following events occur:

- An error message in the following format is displayed:  

```
%IGMP-3-QUERY_INT_MISMATCH: Received a non-matching query interval <interval in seconds>, from querier address <ip-address>
```
- If the query interval on the lower version IGMP-enabled interface has not been modified, the default query interval appears under its respective interface configuration.
- If the query interval on the IGMP-enabled interface has been modified, the configured query interval is updated to show the configured query interval under its respective interface configuration.

**Note**

The **show ip igmp interface** command displays both the configured query interval and the received query interval in its output.

Be careful when increasing the query interval in an environment with IGMPv2 routers (the default) and Layer 2 (L2) snooping switches: An IGMPv2 snooping switch needs to know the query interval of the IGMP querier, because it is not signaled in IGMP messages (in IGMPv3 it is). The IGMP snooping switch times out membership state based on what it thinks the query interval is. If the querier uses a query interval larger than what the IGMP snooping switch assumes, then this may lead to an unexpected timeout of multicast state on the IGMP snooping switch.

**Note**

The default IGMP query interval on Cisco routers of 60 seconds is never an issue with Cisco IGMP snooping switches because they either assume a 60 second-interval or tries to determine the query interval by measuring the interval between IGMP general queries.

Be careful decreasing the query interval because it increases the processing load on the router (total number of IGMP reports received over a period of time)—especially on routers with a large number of interfaces and hosts connected to it (for example, a broadband aggregation router).

If the IGMP query interval and IGMP querier timeout period are modified on an interface, the following conditions apply:

- By default, if the query interval is modified using the **ip igmp query-interval** command, the timeout period automatically adjusts to two times the query interval; the adjusted timeout period, however, is *not* be reflected in the interface configuration.
  - To confirm that the timeout period adjusted to two times the modified query interval, you can use the **show ip igmp interface** command; the output for this command displays the IGMP query interval and timeout period being used for the interface.
  - If you would like to have the ability to view the modified IGMP querier timeout period in the interface configuration, you can manually configure the timeout period using the **ip igmp querier-timeout** command. For the *seconds* argument, specify a value that is two times the modified query interval.
- If the timeout period is modified using the **ip igmp querier-timeout** command, the query interval does *not* automatically adjust to be in proportion with the modified timeout period (half of the timeout period), so it is possible to override the default timeout period of two times the query interval.

**Note**

If the timeout period is modified for the **ip igmp querier-timeout** command, we recommend that it be changed in proportion to the IGMP query interval.

- If the IGMP query interval is modified, the modified query interval must be greater than the IGMP maximum query response time (which is controlled using the **ip igmp max-response-time** command).

### Examples

The following example shows how to increase the frequency at which the IGMP querier sends IGMP host-query messages to 120 seconds. The IGMP timeout period automatically adjusts to two times the configured query interval (240 seconds, in this example).

```
interface tunnel 0
 ip igmp query-interval 120
```

### Related Commands

| Command                          | Description                                                                                          |
|----------------------------------|------------------------------------------------------------------------------------------------------|
| <b>ip igmp max-response-time</b> | Configures the maximum response time advertised in IGMP queries.                                     |
| <b>show ip igmp interface</b>    | Displays information about the status and configuration of IGMP and multicast routing on interfaces. |

# ip igmp query-max-response-time

To configure the maximum response time advertised in Internet Group Management Protocol (IGMP) queries, use the **ip igmp query-max-response-time** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**ip igmp query-max-response-time** *seconds*

**no ip igmp query-max-response-time**

| Syntax Description | <i>seconds</i> | Maximum response time, in seconds, advertised in IGMP queries. The default value is 10 seconds. |
|--------------------|----------------|-------------------------------------------------------------------------------------------------|
|--------------------|----------------|-------------------------------------------------------------------------------------------------|

| Command Default | <i>seconds</i> : 10 seconds |
|-----------------|-----------------------------|
|-----------------|-----------------------------|

| Command Modes | Interface configuration |
|---------------|-------------------------|
|---------------|-------------------------|

| Command History | Release     | Modification                                                                                                                                                                      |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 11.1        | This command was introduced.                                                                                                                                                      |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                 | 12.2(33)MRB | This command was integrated into Cisco IOS Release 12.2(33)MRB.                                                                                                                   |

| Usage Guidelines | This command is valid only when IGMP Version 2 is running.<br><br>This command controls the period during which the responder can respond to an IGMP query message before the router deletes the group. |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| Examples | The following example configures a maximum response time of 8 seconds:<br><br>ip igmp query-max-response-time 8 |
|----------|-----------------------------------------------------------------------------------------------------------------|
|----------|-----------------------------------------------------------------------------------------------------------------|

| Related Commands | Command                      | Description                                                                                                 |
|------------------|------------------------------|-------------------------------------------------------------------------------------------------------------|
|                  | <b>ip pim query-interval</b> | Configures the frequency of PIM router query messages.                                                      |
|                  | <b>show ip igmp groups</b>   | Displays the multicast groups that are directly connected to the router and that were learned through IGMP. |

# ip igmp static-group

To configure static group membership entries on an interface, use the **ip igmp static-group** command in interface configuration mode. To delete static group membership entries, use the **no** form of this command.

**ip igmp static-group** {*group-address* [**source** {*source-address*}]}

**no ip igmp static-group** {*group-address* [**source** {*source-address*}]}

## Syntax Description

|                       |                                                                                    |
|-----------------------|------------------------------------------------------------------------------------|
| <i>group-address</i>  | IP multicast group address to configure as a static group member on the interface. |
| <b>source</b>         | (Optional) Statically forwards a (S, G) channel out of the interface.              |
| <i>source-address</i> | (Optional) IP address of a system where multicast data packets originate.          |

## Command Default

No static group membership entries are configured on interfaces.

## Command Modes

Interface configuration (config-if)

## Command History

| Release                  | Modification                                                                                                                                         |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.2                     | This command was introduced.                                                                                                                         |
| 12.3(2)T                 | This command was modified. The <b>ssm-map</b> keyword was added.                                                                                     |
| 12.2(18)S                | This command was modified. The <b>ssm-map</b> keyword was added.                                                                                     |
| 12.2(18)SXD3             | This command was integrated into Cisco IOS Release 12.2(18)SXD3.                                                                                     |
| 12.2(27)SBC              | This command was integrated into Cisco IOS Release 12.2(27)SBC.                                                                                      |
| 12.2(18)SXF5             | This command was modified. The <b>class-map</b> keyword and <i>class-map-name</i> argument were added.                                               |
| 15.0(1)M                 | This command was modified. The <b>class-map</b> keyword and <i>class-map-name</i> argument were added.                                               |
| 12.2(33)SRE              | This command was modified. The <b>class-map</b> keyword and <i>class-map-name</i> argument were added.                                               |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6.                                                                                           |
| 12.2(33)MRB              | This command was integrated into Cisco IOS Release 12.2(33)MRB. This release does not support the *, <b>ssm-map</b> , and <b>class-map</b> keywords. |

## Usage Guidelines

Use the **ip igmp static-group** command to configure static group membership entries on an interface. When you configure the **ip igmp static-group** command, packets to the group are fast-switched out the interface, provided that packets were received on the correct reverse path forwarding (RPF) interface. Once configured, static group membership entries are added to the IGMP cache and mroute table.



Configuring the **ip igmp static-group** command is unlike configuring the **ip igmp join-group** command, which allows the router to join the multicast group. This configuration of the **ip igmp static-group** command would cause the upstream routers to maintain the multicast routing table information for that group, which would ensure that all the paths to that multicast group are active.

If you configure the **ip igmp join-group** command for the same group address as the **ip igmp static-group** command, the **ip igmp join-group** command takes precedence, and the group behaves like a locally joined group.

---

**Examples**

The following example shows how to configure group address 239.100.100.101 on Ethernet interface 0:

```
interface ethernet 0
 ip igmp static-group 239.100.100.101
```

---

**Related Commands**

| Command                   | Description                                  |
|---------------------------|----------------------------------------------|
| <b>ip igmp join-group</b> | Causes the router to join a multicast group. |

# ip igmp version

To configure which version of Internet Group Management Protocol (IGMP) the router uses, use the **ip igmp version** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**ip igmp version {1 | 2 | 3}**

**no ip igmp version**

## Syntax Description

|          |                                      |
|----------|--------------------------------------|
| <b>1</b> | IGMP Version 1.                      |
| <b>2</b> | IGMP Version 2. This is the default. |
| <b>3</b> | IGMP Version 3.                      |

## Command Default

Version 2

## Command Modes

Interface configuration

## Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.1        | This command was introduced.                                                                                                                                                      |
| 12.1(5)T    | The <b>3</b> keyword was added.                                                                                                                                                   |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)MRB | This command was integrated into Cisco IOS Release 12.2(33)MRB.                                                                                                                   |

## Usage Guidelines

All routers on the subnet must support the same version. The router does not automatically detect Version 1 routers and switch to Version 1 as did earlier releases of the Cisco IOS software. Hosts can have any IGMP version (1, 2, or 3) and the router correctly detects their presence and query them appropriately.

Some commands require IGMP Version 2 or 3, such as the **ip igmp query-max-response-time** and **ip igmp query-timeout** commands.

## Examples

The following example configures the router to use IGMP Version 3:

```
ip igmp version 3
```

## Related Commands

| Command                                | Description                                                                                                 |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------|
| <b>ip igmp query-max-response-time</b> | Configures the maximum response time advertised in IGMP queries.                                            |
| <b>show ip igmp groups</b>             | Displays the multicast groups that are directly connected to the router and that were learned through IGMP. |
| <b>show ip igmp interface</b>          | Displays multicast-related information about an interface.                                                  |

# ip local interface

To configure the IP address of the provider edge (PE) router interface to be used as the source IP address for sending tunneled packets, use the **ip local interface** command in pseudowire-class configuration mode. To remove the IP address, use the **no** form of this command.

**ip local interface** *interface-name*

**no ip local interface** *interface-name*

## Syntax Description

|                       |                                                                                                                            |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
| <i>interface-name</i> | Name of the PE interface whose IP address is used as the source IP address for sending tunneled packets over a Layer 2 PW. |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------|

## Command Default

No IP address is configured.

## Command Modes

Pseudowire-class configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(19)MR2 | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

Use the same local interface name for all pseudowire-classes configured between a pair of PE routers. It is highly recommended that you configure a loopback interface with this command. If you do not, the router chooses the “best available local address,” which could be any IP address configured on a core-facing interface. This configuration could prevent a control channel from being established.

## Examples

The following example shows how to configure the IP address of the local loopback 0 as the source IP address for sending packets through an MPLS session:

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# ip local interface loopback 0
Router(config-pw-class)# exit
Router(config)# exit
```

## Related Commands

| Command             | Description                                                                                                                                             |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ima-group</b>    | Configures the physical links as IMA group members, which executes the interface configuration command for each physical link included in an IMA group. |
| <b>ima group-id</b> | Enables the user to configure the IMA Group ID for the IMA interface.                                                                                   |

| Command                       | Description                                                                            |
|-------------------------------|----------------------------------------------------------------------------------------|
| <b>interface atm</b>          | Configures physical links for an ATM interface.                                        |
| <b>show ima interface atm</b> | Displays general and detailed information about IMA groups and the links they include. |

# ip multicast-routing

To enable IP multicast routing, use the **ip multicast-routing** command in global configuration mode. To disable IP multicast routing, use the **no** form of this command.

**ip multicast-routing** [**vrf** *vrf-name*]

**no ip multicast-routing** [**vrf** *vrf-name*]

|                           |                            |                                                                                                                                                                            |
|---------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>vrf</b> <i>vrf-name</i> | (Optional) Enables IP multicast routing for the Multicast Virtual Private Network (VPN) routing and forwarding (MVRP) instance specified for the <i>vrf-name</i> argument. |
|---------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                        |                                   |
|------------------------|-----------------------------------|
| <b>Command Default</b> | IP multicast routing is disabled. |
|------------------------|-----------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                                                                                                                                                                              |
|------------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | 10.0           | This command was introduced.                                                                                                                                                                                                                                                                     |
|                        | 11.2(11)GS     | The distributed keyword was added.                                                                                                                                                                                                                                                               |
|                        | 12.0(5)T       | The effect of this command was modified. If IP multicast Multilayer Switching (MLS) is enabled, using the no form of this command now disables IP multicast routing on the Multicast MultiLayer Switching (MMLS) route processor (RP) and purges all multicast MLS cache entries on the MMLS-SE. |
|                        | 12.0(23)S      | The vrf keyword and vrf-name argument were added.                                                                                                                                                                                                                                                |
|                        | 12.2(13)T      | The vrf keyword and vrf-name argument were added.                                                                                                                                                                                                                                                |
|                        | 12.2(14)S      | This command was integrated into Cisco IOS Release 12.2(14)S.                                                                                                                                                                                                                                    |
|                        | 12.2(18)SXE    | Support for this command was introduced on the Supervisor Engine 720.                                                                                                                                                                                                                            |
|                        | 12.2(27)SBC    | This command was integrated into Cisco IOS Release 12.2(27)SBC.                                                                                                                                                                                                                                  |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                                                                                                                                  |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                                                                                                                                   |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA. The command was only supported for use with PTP redundancy.                                                                                                                                                                      |
|                        | 12.2(33)MRB    | This command was integrated into Cisco IOS Release 12.2(33)MRB. This release does not support the <b>distributed</b> keyword.                                                                                                                                                                    |

|                         |                                                                                                       |
|-------------------------|-------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | When IP multicast routing is disabled, the Cisco IOS software does not forward any multicast packets. |
|-------------------------|-------------------------------------------------------------------------------------------------------|

---

**Examples**

The following example shows how to enable IP multicast routing:

```
Router(config)# ip multicast-routing
```

The following example shows how to enable IP multicast routing for a specific VRF:

```
Router(config)# ip multicast-routing vrf vrf1
```

The following example shows how to disable IP multicast routing:

```
Router(config)# no ip multicast-routing
```

---

**Related Commands**

| Command       | Description                  |
|---------------|------------------------------|
| <b>ip pim</b> | Enables PIM on an interface. |

# ip ospf bfd

To enable Bidirectional Forwarding Detection (BFD) on a specific interface configured for Open Shortest Path First (OSPF), use the **ip ospf bfd** command in interface configuration mode. To disable BFD on the OSPF interface, use the **disable** keyword. To remove the **ip ospf bfd** command, use the **no** form of this command.

**ip ospf bfd [disable]**

**no ip ospf bfd**

|                           |                                                                           |
|---------------------------|---------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>disable</b> (Optional) Disables BFD for OSPF on a specified interface. |
|---------------------------|---------------------------------------------------------------------------|

|                        |                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Command Default</b> | When the <b>disable</b> keyword is not used, the default behavior is to enable BFD support for OSPF on the interface. |
|------------------------|-----------------------------------------------------------------------------------------------------------------------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | Interface configuration |
|----------------------|-------------------------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(18)SXE | This command was introduced.                                    |
|                 | 12.0(31)S   | This command was integrated into Cisco IOS Release 12.0(31)S.   |
|                 | 12.4(4)T    | This command was integrated into Cisco IOS Release 12.4(4)T.    |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | Enter the <b>ip ospf bfd</b> command to configure an OSPF interface to use BFD for failure detection. If you have used the <b>bfd-all interfaces</b> command in router configuration mode to globally configure all OSPF interfaces for an OSPF process to use BFD, you can enter the <b>ip ospf bfd</b> command in interface configuration mode with the <b>disable</b> keyword to disable BFD for a specific OSPF interface. |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                                                                                   |
|-----------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | In the following example, the interface associated with OSPF, Fast Ethernet interface 3/0, is configured for BFD: |
|-----------------|-------------------------------------------------------------------------------------------------------------------|

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 3/0
Router(config-if)# ip ospf bfd
Router(config-if)# end
```



| Related Commands | Command                   | Description                                    |
|------------------|---------------------------|------------------------------------------------|
|                  | <b>bfd all-interfaces</b> | Enables BFD for all interfaces for a BFD peer. |

# ip pim

To enable Protocol Independent Multicast (PIM) on an interface, use the **ip pim** command in interface configuration mode. To disable PIM on the interface, use the **no** form of this command.

**ip pim** { **dense-mode** [**proxy-register** {**list** *access-list* | **route-map** *map-name*}] | **passive** | **sparse-mode** | **sparse-dense-mode** }

**no ip pim** { **dense-mode** [**proxy-register** {**list** *access-list* | **route-map** *map-name*}] | **passive** | **sparse-mode** | **sparse-dense-mode** }

## Syntax Description

|                                  |                                                                                                                                                                                                |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dense-mode</b>                | Enables dense mode of operation.                                                                                                                                                               |
| <b>proxy-register</b>            | (Optional) Enables proxy registering on the interface of a designated router (DR) (leading toward the bordering dense mode region) for multicast traffic from sources not connected to the DR. |
| <b>list</b> <i>access-list</i>   | (Optional) Defines the extended access list number or name.                                                                                                                                    |
| <b>route-map</b> <i>map-name</i> | (Optional) Defines the route map.                                                                                                                                                              |
| <b>passive</b>                   | Enables passive mode of operation                                                                                                                                                              |
| <b>sparse-mode</b>               | Enables sparse mode of operation.                                                                                                                                                              |
| <b>sparse-dense-mode</b>         | Treats the interface in either sparse mode or dense mode of operation, depending on which mode the multicast group operates in.                                                                |

## Command Default

IP multicast routing is disabled on all interfaces.

## Command Modes

Interface configuration

## Command History

| Release     | Modification                                                                                                                                                                                                     |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.0        | This command was introduced.                                                                                                                                                                                     |
| 11.1        | The <b>sparse-dense-mode</b> keyword was added.                                                                                                                                                                  |
| 12.0S       | The following keywords and arguments were added: <ul style="list-style-type: none"> <li>• <b>proxy-register</b></li> <li>• <b>list</b> <i>access-list</i></li> <li>• <b>route-map</b> <i>map-name</i></li> </ul> |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                                                  |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.                                |
| 12.2(33)SRE | This command was modified. The <b>passive</b> keyword was added.                                                                                                                                                 |
| 12.2(33)MRB | This command was integrated into Cisco IOS Release 12.2(33)MRB. The <b>dense</b> , <b>proxy-register</b> , and <b>list</b> keywords are not supported.                                                           |

## Usage Guidelines

Enabling PIM on an interface also enables Internet Group Management Protocol (IGMP) operation on that interface. An interface can be configured to be in dense mode, passive mode, sparse mode, or sparse-dense mode. The mode describes how the Cisco IOS software populates its multicast routing table and how the software forwards multicast packets it receives from its directly connected LANs. Dense mode interfaces are always added to the table when the multicast routing table is populated. Sparse mode interfaces are added to the table only when periodic join messages are received from downstream routers, or there is a directly connected member on the interface.

### Dense Mode

Initially, a dense mode interface forwards multicast packets until the router determines that there are group members or downstream routers, or until a prune message is received from a downstream router. Then, the dense mode interface periodically forwards multicast packets out the interface until the same conditions occur. Dense mode assumes that multicast group members are present. Dense mode routers never send a join message. They do send prune messages as soon as they determine they have no members or downstream PIM routers. A dense mode interface is subject to multicast flooding by default.

### Dense Mode with Proxy Registering

For a router in a PIM sparse mode (PIM-SM) domain configured to operate in sparse mode or sparse-dense mode, the **ip pim dense-mode proxy-register** command must be configured on the interface leading toward the bordering dense mode region. This configuration enables the router to register traffic from the dense mode region with the rendezvous point (RP) in the sparse mode domain.

Prior to Cisco IOS Release 12.0 S, an RP needed to be running on the border router leading toward a dense mode region so that the RP could learn about traffic from sources in the dense mode region.

This command requires an extended access list or route map argument specifying which traffic the router needs to register with the RP. This command applies only to sources reachable through a PIM router. Cisco IOS software always registers traffic from remote sources if it arrives on a dense mode interface and if the Reverse Path Forwarding (RPF) neighbor leading toward the source is a Distance Vector Multicast Routing Protocol (DVMRP) but not a PIM router. This functionality has existed since Cisco IOS Release 10.0 and cannot be modified (restricted) with an access list or route map.

### Passive Mode

An interface configured with passive mode does not pass or forward PIM control plane traffic; it passes or forwards only IGMP traffic. If passive mode is configured on an interface enabled for IP multicast, the router does not send PIM messages on the interface nor does it accept PIM messages from other routers on this interface. The router acts as the only PIM router on the network and works as the designated router (DR) and the designated forwarder (DF) for all Bidirectional PIM group ranges.

The **ip pim neighbor-filter** command has no effect and is superseded by the **ip pim passive** command when both commands are configured on the same interface.

Do not use the **ip pim passive** command on LANs that have more than one IP multicast router connected to them, because all routers with this command become DR and DF, resulting in duplicate traffic (PIM-SM, PIM-DM, PIM-SSM) or looping traffic (Bidir-PIM). To limit PIM messages to and from valid routers on LANs with more than one router, use the **ip pim neighbor-filter** command.

### Sparse Mode

A sparse mode interface is used for multicast forwarding only if a join message is received from a downstream router or if group members are directly connected to the interface. Sparse mode assumes that no other multicast group members are present. When sparse mode routers want to join the shared path, they periodically send join messages toward the RP. When sparse mode routers want to join the source path, they periodically send join messages toward the source; they also send periodic prune messages toward the RP to prune the shared path.

### Sparse-Dense Mode

An alternative to choosing just dense mode or just sparse mode is to run PIM in a single region in sparse mode for some groups and dense mode for other groups.

In sparse-dense mode, if the group is in dense mode, the interface is treated as dense mode. If the group is in sparse mode, the interface is treated in sparse mode. The group is “sparse” if the router knows about an RP for that group.

When an interface is treated in dense mode, it is populated in the outgoing interface list of the multicast routing table when either of the following conditions is true:

- Members or DVMRP neighbors are on the interface.
- Any of the PIM neighbors on the interface have not pruned for the group.

When an interface is treated in sparse mode, it is populated in the outgoing interface list of the multicast routing table when either of the following conditions is true:

- Members or DVMRP neighbors are on the interface.
- A PIM neighbor on the interface has received an explicit join message.

### Examples

The following example shows how to enable PIM-SM on tunnel interface 0 and set the address of the RP router to 226.0.0.8:

```
ip pim rp-address 226.0.0.8
interface tunnel 0
 ip pim sparse-mode
```

The following example shows how to enable PIM dense mode (PIM-DM) on Ethernet interface 1:

```
interface ethernet 1
 ip pim dense-mode
```

The following example shows how to enable PIM sparse-dense mode on Ethernet interface 1:

```
interface ethernet 1
 ip pim sparse-dense-mode
```

The following example shows how to register the multicast traffic for any source and any multicast group:

```
interface ethernet 0
 ip address 172.16.0.0 255.255.255.0
 description Ethernet interface towards the PIM sparse-mode domain
 ip pim sparse-dense-mode
!
interface ethernet 1
 ip address 192.44.81.5 255.255.255.0
 description Ethernet interface towards the PIM dens-mode region
 ip pim dense-mode proxy-register list 100
!
access-list 100 permit ip any any
```

### Related Commands

| Command                       | Description                                                      |
|-------------------------------|------------------------------------------------------------------|
| <b>ip multicast-routing</b>   | Enables IP multicast routing or multicast distributed switching. |
| <b>ip pim neighbor-filter</b> | Filters PIM messages.                                            |

| Command                      | Description                                                |
|------------------------------|------------------------------------------------------------|
| <b>ip pim rp-address</b>     | Configures the address of a PIM RP for a particular group. |
| <b>show ip pim interface</b> | Displays information about interfaces configured for PIM.  |

# ip pim bsr-border

To prevent bootstrap router (BSR) messages from being sent or received through an interface, use the **ip pim bsr-border** command in interface configuration mode. To disable this configuration, use the **no** form of this command.

**ip pim bsr-border**

**no ip pim bsr-border**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The command is disabled.

**Command Modes** Interface configuration

## Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.3 T      | The <b>ip pim border</b> command was introduced.                                                                                                                                  |
| 12.0(8)     | The <b>ip pim border</b> command was replaced by the <b>ip pim bsr-border</b> command.                                                                                            |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)MRB | This command was integrated into Cisco IOS Release 12.2(33)MRB.                                                                                                                   |

## Usage Guidelines

When this command is configured on an interface, no Protocol Independent Multicast (PIM) Version 2 BSR messages are sent or received through the interface. Configure an interface bordering another PIM domain with this command to avoid BSR messages from being exchanged between the two domains. BSR messages should not be exchanged between different domains, because routers in one domain may elect rendezvous points (RPs) in the other domain, resulting in protocol malfunction or loss of isolation between the domains.



### Note

This command does not set up multicast boundaries. It sets up only a PIM domain BSR message border.

## Examples

The following example configures the interface to be the PIM domain border:

```
interface ethernet 1
ip pim bsr-border
```

**Related Commands**

| Command                      | Description                                               |
|------------------------------|-----------------------------------------------------------|
| <b>show ip pim interface</b> | Displays information about interfaces configured for PIM. |

# ip pim bsr-candidate

To configure the router to announce its candidacy as a bootstrap router (BSR), use the **ip pim bsr-candidate** command in global configuration mode. To remove this router as a candidate for being a bootstrap router, use the **no** form of this command.

**ip pim** [**vrf** *vrf-name*] **bsr-candidate** *interface-type interface-number* [*hash-mask-length*] [*priority*]

**no ip pim** [**vrf** *vrf-name*] **bsr-candidate** *interface-type interface-number* [*hash-mask-length*] [*priority*]

## Syntax Description

|                                        |                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vrf</b>                             | (Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.                                                                                                                                                                                                                                       |
| <i>vrf-name</i>                        | (Optional) Name assigned to the VRF.                                                                                                                                                                                                                                                                                                         |
| <i>interface-type interface-number</i> | Interface type and number on this router from which the BSR address is derived, to make it a candidate. This interface must be enabled with Protocol Independent Multicast (PIM).                                                                                                                                                            |
| <i>hash-mask-length</i>                | (Optional) Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash (correspond) to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This fact allows you to get one RP for multiple groups. |
| <i>priority</i>                        | (Optional) Priority of the candidate BSR. Integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR. The default value is 0.                                                                                                               |

## Command Default

The command is disabled.  
*priority*: 0



### Note

The Cisco IOS implementation of PIM BSR uses the value 0 as the default priority for candidate RPs and BSRs. This implementation predates the draft-ietf-pim-sm-bsr IETF draft, the first IETF draft to specify 192 as the default priority value. The Cisco IOS implementation, thus, deviates from the IETF draft. To comply with the default priority value specified in the draft, you must explicitly set the priority value to 192.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                          |
|-------------|-----------------------------------------------------------------------|
| 11.3T       | This command was introduced.                                          |
| 12.0(23)S   | The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.       |
| 12.2(13)T   | The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.       |
| 12.2(14)S   | This command was integrated into Cisco IOS Release 12.2(14)S.         |
| 12.2(18)SXE | Support for this command was introduced on the Supervisor Engine 720. |



| Release      | Modification                                                    |
|--------------|-----------------------------------------------------------------|
| 12.2(27)SBC  | This command was integrated into Cisco IOS Release 12.2(27)SBC. |
| 12.2(33)SRA  | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)MRB. | This command was integrated into Cisco IOS Release 12.2(33)MRB. |

## Usage Guidelines

This command causes the router to send bootstrap messages to all its PIM neighbors, with the address of the designated interface as the BSR address. Each neighbor compares the BSR address with the address it had from previous bootstrap messages (not necessarily received on the same interface). If the current address is the same or higher address, it caches the current address and forwards the bootstrap message. Otherwise, it drops the bootstrap message.

This router continues to be the BSR until it receives a bootstrap message from another candidate BSR saying that it has a higher priority (or if the same priority, a higher IP address).

Use this command only in backbone routers that have good connectivity to all parts of the PIM domain. That is, a stub router that relies on an on-demand dialup link to connect to the rest of the PIM domain is not a good candidate BSR.

You must enable the *interface-type* with PIM.

When you set the *hash-mask-length* argument, all groups with the same seed hash correspond to the same rendezvous point. For example, if this value is 24, only the first 24 bits of the group addresses are applicable; using this setting allows you to get one rendezvous point for multiple groups.

When you set the *priority* argument, the BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR.

## Examples

The following example shows how to configure the IP address of the router on Ethernet interface 0/0 to be a candidate BSR with a priority of 192:

```
ip pim bsr-candidate ethernet 0/0 192
```

## Related Commands

| Command                         | Description                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------|
| <b>ip pim rp-candidate</b>      | Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR. |
| <b>ip pim send-rp-discovery</b> | Configures the router to be an RP-mapping agent.                                      |

# ip pim query-interval

To configure the frequency of Protocol Independent Multicast (PIM) query (hello) messages, use the **ip pim query-interval** command in interface configuration mode. To return to the default interval, use the **no** form of this command.

**ip pim query-interval** *period* [msec]

**no ip pim query-interval**

|                           |               |                                                                                                                                                                                                                                                |
|---------------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>period</i> | The number of seconds or milliseconds (ms) that can be configured for the PIM hello (query) interval. The range is from 1 to 65535.                                                                                                            |
|                           | <b>msec</b>   | (Optional) Specifies that the interval configured for the <i>period</i> argument be interpreted in milliseconds. If the <b>msec</b> keyword is not used along with the <i>period</i> argument, the interval range is assumed to be in seconds. |

**Command Default** PIM hello (query) messages are sent every 30 seconds.

**Command Modes** Interface configuration

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                                                               |
|------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        |                |                                                                                                                                                                                   |
|                        | 10.0           | This command was introduced.                                                                                                                                                      |
|                        | 12.0(22)S      | The <b>msec</b> keyword was added.                                                                                                                                                |
|                        | 12.2(14)S      | This command was integrated into Cisco IOS Release 12.2(14)S.                                                                                                                     |
|                        | 12.2(15)T      | This command was integrated into Cisco IOS Release 12.2(15)T.                                                                                                                     |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                        | 12.2(31)SB     | This command was integrated into Cisco IOS Release 12.2(31)SB.                                                                                                                    |
|                        | 12.2SX         | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                        | 12.2(33)MRB    | This command was integrated into Cisco IOS Release 12.2(33)MRB.                                                                                                                   |

**Usage Guidelines** Use this command to configure the frequency of PIM neighbor discovery messages. By default these messages are sent once every 30 seconds. In PIM Version 1 (PIMv1), these messages are referred to as PIM query messages; in PIM Version 2 (PIMv2), these messages are referred to as PIM hello messages. By default, routers run PIMv2 and send PIM hello messages. A router changes (auto-fallback) to PIMv1 and sends PIM query messages if it detects a neighboring router that only supports PIMv1. As soon as that neighboring PIMv1 router is removed from the network, the router reverts to PIMv2.



**Note**

A router can be configured to exclusively use PIMv1 on an interface with the **ip pim version 1** command.

**Note**

In PIM version 2, PIM hello messages also contain a variety of options that allow PIM routers on the network to learn about the capabilities of PIM neighbors. For more information about these capabilities, see the **show ip pim neighbor** command page.

PIM neighbor discovery messages are used to determine which router on a network is acting as the Designated Router (DR) for PIM sparse mode (PIM-SM) and Source Specific Multicast (SSM). The DR is responsible for joining PIM-SM and SSM groups receiving multicast traffic from sources requested by receivers (hosts). In addition, in PIM-SM, the DR is also responsible for registering local sources with the RP. If the DR fails, a backup router becomes the DR and then forward traffic for local receivers and register local sources.

The *period* argument is used to specify the PIM hello (query) interval. The interval determines the frequency at which PIM hello (query) messages are sent.

**Note**

When an interface enabled for PIM comes up, a PIM hello (query) message is sent immediately. In some cases, the initial PIM hello (query) message may be lost. If the first PIM hello (query) does not get sent when an interface initially comes up, another is sent 3 seconds later regardless of the PIM hello (query) interval to ensure that there are no initialization delays.

The configured PIM hello interval also determines the holdtime used by a PIM router. The Cisco IOS software calculates the holdtime as follows:

$3 * \text{the interval specified for the } period \text{ argument}$

By default, PIM routers announce the holdtime in PIM hello (query) messages. If the holdtime expires and another router has not received another hello (query) message from this router, it times out the PIM neighbor. If the timed out router was the DR, the timeout triggers DR election. By default, the DR-failover interval occurs after 90 seconds (after the default holdtime expires for a DR). To reduce DR-failover time in redundant networks, a lower value for the *period* argument can be configured on all routers. The minimum DR-failover time that can be configured (in seconds) is 3 seconds (when the *period* argument is set to 1 second). The DR-failover time can be reduced to less than 3 seconds if the **msecs** keyword is specified. When the **msecs** keyword is used with the **ip pim query-interval** command, the value specified for the *period* argument is interpreted as a value in milliseconds (instead of seconds). By enabling a router to send PIM hello messages more often, this functionality allows the router to discover unresponsive neighbors more quickly. As a result, the router can implement failover or recovery procedures more efficiently.

**Note**

If IGMP Version 1 is being used on a network, then the DR is also the IGMP querier; if at least IGMP version 2 is being used, then the router with the lowest IP address becomes the IGMP querier.


**Examples**

The following example shows how to set the PIM hello interval to 45 seconds:

```
interface FastEthernet0/1
 ip pim query-interval 45
```

The following example shows how to set the PIM hello interval to 100 milliseconds:

```
interface FastEthernet0/1
 ip pim query-interval 100 msec
```

 ip pim query-interval

| Related Commands | Command              | Description                                                                                                |
|------------------|----------------------|------------------------------------------------------------------------------------------------------------|
|                  | show ip pim neighbor | Displays information about PIM neighbors discovered by PIMv1 router query messages or PIMv2 hello messages |

# ip pim register-source

To configure the IP source address of a register message to an interface address other than the outgoing interface address of the designated router (DR) leading toward the rendezvous point (RP), use the **ip pim register-source** command in global configuration mode. To disable this configuration, use the **no** form of this command.

**ip pim** [**vrf** *vrf-name*] **register-source** *interface-type interface-number*

**no ip pim** [**vrf** *vrf-name*] **register-source**

| Syntax Description                               |                                                                                                        |  |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------|--|
| <b>vrf</b>                                       | (Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance. |  |
| <i>vrf-name</i>                                  | (Optional) Name assigned to the VRF.                                                                   |  |
| <i>interface-type</i><br><i>interface-number</i> | Interface type and interface number that identify the IP source address of a register message.         |  |

| Command Default | By default, the IP address of the outgoing interface of the DR leading toward the RP is used as the IP source address of a register message. |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------|
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------|

| Command Modes | Global configuration |
|---------------|----------------------|
|---------------|----------------------|

| Command History | Release     | Modification                                                          |
|-----------------|-------------|-----------------------------------------------------------------------|
|                 | 12.0(8)T    | This command was introduced.                                          |
|                 | 12.0(23)S   | The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.       |
|                 | 12.2(13)T   | The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.       |
|                 | 12.2(14)S   | This command was integrated into Cisco IOS Release 12.2(14)S.         |
|                 | 12.2(18)SXE | Support for this command was introduced on the Supervisor Engine 720. |
|                 | 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC.       |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.       |
|                 | 12.2(33)MRB | This command was integrated into Cisco IOS Release 12.2(33)MRB.       |

| Usage Guidelines | This command is required only when the IP source address of a register message is not a uniquely routed address to which the RP can send packets. This situation may occur if the source address is filtered such that packets sent to it are not forwarded or if the source address is not unique to the network. In these cases, the replies sent from the RP to the source address fails to reach the DR, resulting in Protocol Independent Multicast sparse mode (PIM-SM) protocol failures. |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

If no IP source address is configured or if the configured source address is not in service, the IP address of the outgoing interface of the DR leading toward the RP is used as the IP source address of the register message. Therefore, we recommend using a loopback interface with an IP address that is uniquely routed throughout the PIM-SM domain.

---

**Examples**

The following example shows how to configure the IP source address of the register message to the loopback 3 interface of a DR:

```
ip pim register-source loopback 3
```

# ip pim rp-address

To statically configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for multicast groups, use the **ip pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

**ip pim rp-address** *rp-address* [*access-list*] [**override**]

**no ip pim rp-address** *rp-address* [*access-list*] [**override**]

|                           |                    |                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>rp-address</i>  | IP address of the RP to be used for the static group-to-RP mapping. This is a unicast IP address in four-part dotted-decimal notation.                                                                                                                                                                                                                                                        |
|                           | <i>access-list</i> | (Optional) Number or name of a standard access list that defines the multicast groups to be statically mapped to the RP.<br><br><b>Note</b> If no access list is defined, the RP maps to all multicast groups, 224/4.                                                                                                                                                                         |
|                           | <b>override</b>    | (Optional) Specifies that if dynamic and static group-to-RP mappings are used together and there is an RP address conflict, the RP address configured for a static group-to-RP mapping takes precedence.<br><br><b>Note</b> If the <b>override</b> keyword is not specified and there is RP address conflict, dynamic group-to-RP mappings takes precedence over static group-to-RP mappings. |
|                           |                    |                                                                                                                                                                                                                                                                                                                                                                                               |

**Command Default** No PIM static group-to-RP mappings are configured.

**Command Modes** Global configuration (config)

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                                                               |
|------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | 10.2           | This command was introduced.                                                                                                                                                      |
|                        | 11.1           | The <b>override</b> keyword was added.                                                                                                                                            |
|                        | 12.1(2)T       | The <b>bidir</b> keyword was added.                                                                                                                                               |
|                        | 12.0(23)S      | The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.                                                                                                                   |
|                        | 12.2(13)T      | The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.                                                                                                                   |
|                        | 12.2(14)S      | This command was integrated into Cisco IOS Release 12.2(14)S.                                                                                                                     |
|                        | 12.2(27)SBC    | This command was integrated into Cisco IOS Release 12.2(27)SBC.                                                                                                                   |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                        | 12.2SX         | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

| Release     | Modification                                                                                                                            |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. The command was only supported for use with PTP redundancy.             |
| 12.2(33)MRB | This command was integrated into Cisco IOS Release 12.2(33)MRB. This release does not support the <b>vrf</b> and <b>bidir</b> keywords. |

### Usage Guidelines

In the Cisco IOS implementation of PIM, each multicast group individually operates in one of the following modes: dense mode, sparse mode, or bidirectional mode. Groups in sparse mode (PIM-SM) or bidirectional mode (bidir-PIM) use RPs to connect sources and receivers. All routers in a PIM domain need to have a consistent configuration for the mode and RP addresses of the multicast groups.

The Cisco IOS software learns the mode and RP addresses of multicast groups through the following three mechanisms: static group-to-RP mapping configurations, Auto-RP, and bootstrap router (BSR). By default, groups operate in dense mode. No commands explicitly define groups to operate in dense mode.

Use the **ip pim rp-address** command to statically define the RP address for PIM-SM or bidir-PIM groups (an **ip pim rp-address** command configuration is referred to as a static group-to-RP mapping).

You can configure a single RP for more than one group using an access list. If no access list is specified, the static RP maps to all multicast groups, 224/4.

You can configure multiple RPs, but only one RP per group range.

If multiple **ip pim rp-address** commands are configured, the following rules apply:

- Highest RP IP address selected regardless of reachability: If a multicast group is matched by the access list of more than one configured **ip pim rp-address** command, then the RP for the group is determined by the RP with the highest RP address configured.
- One RP address per command: If multiple **ip pim rp-address** commands are configured, each static group-to-RP mapping must be configured with a unique RP address (if not, it is overwritten). This restriction also means that only one RP address can be used to provide RP functions for either sparse mode or bidirectional mode groups. If you want to configure static group-to-RP mappings for both bidirectional and sparse mode, the RP addresses must be unique for each mode.
- One access list per command: If multiple **ip pim rp-address** commands are configured, only one access list can be configured per static group-to-RP mapping. An access list cannot be reused with other static group-to-RP mappings configured on a router.

If dynamic and static group-to-RP mappings are used together, the following rule applies to a multicast group: Dynamic group-to-RP mappings take precedence over static group-to-RP mappings—unless the **override** keyword is used.

### Examples

The following example shows how to set the PIM RP address to 192.168.0.1 for all multicast groups (224/4) and defines all groups to operate in sparse mode:

```
ip pim rp-address 192.168.0.1
```



# ip pim rp-candidate

To configure the router to advertise itself to the bootstrap router (BSR) as a Protocol Independent Multicast (PIM) Version 2 candidate rendezvous point (RP), use the **ip pim rp-candidate** command in global configuration mode. To remove this router as an RP candidate, use the **no** form of this command.

**ip pim** [*vrf vrf-name*] **rp-candidate** *interface-type interface-number* [**group-list** *access-list*] [**interval** *seconds*] [**priority** *value*]

**no ip pim** [*vrf vrf-name*] **rp-candidate**

| Syntax Description                               |                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vrf</b>                                       | (Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.                                                                                                                                                                                                            |
| <i>vrf-name</i>                                  | (Optional) Name assigned to the VRF.                                                                                                                                                                                                                                                                              |
| <i>interface-type</i><br><i>interface-number</i> | The IP address associated with this interface type and number is advertised as a candidate RP address.                                                                                                                                                                                                            |
| <b>group-list</b> <i>access-list</i>             | (Optional) Specifies the standard IP access list number or name that defines the group prefixes that are advertised in association with the RP address. The access list name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid confusion with numbered access lists. |
| <b>interval</b> <i>seconds</i>                   | (Optional) Indicates the RP candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.                                                                                                                                                                              |
| <b>priority</b> <i>value</i>                     | (Optional) Indicates the RP priority value. The range is from 0 to 255. The default value is 0.                                                                                                                                                                                                                   |

## Command Default

The command is disabled.

*seconds*: 60

*priority*: 0



### Note

The Cisco IOS implementation of PIM BSR uses the value 0 as the default priority for candidate RPs and BSRs. This implementation predates the draft-ietf-pim-sm-bsr IETF draft, the first IETF draft to specify 192 as the default priority value. The Cisco IOS implementation, thus, deviates from the IETF draft. To comply with the default priority value specified in the draft, you must explicitly set the priority value to 192.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                                                                            |
|-------------|-------------------------------------------------------------------------------------------------------------------------|
| 11.3T       | This command was introduced.                                                                                            |
| 12.1(2)T    | The <b>bidir</b> keyword was added.                                                                                     |
| 12.0(23)S   | The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.                                                         |
| 12.2(13)T   | The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.                                                         |
| 12.2(14)S   | This command was integrated into Cisco IOS Release 12.2(14)S.                                                           |
| 12.2(18)SXE | Support for this command was introduced on the Supervisor Engine 720.                                                   |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC.                                                         |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                         |
| 12.2(33)MRB | This command was integrated into Cisco IOS Release 12.2(33)MRB. This release does not support the <b>bidir</b> keyword. |

## Usage Guidelines

This command causes the router to send a PIM Version 2 message advertising itself as a candidate RP to the BSR. The addresses allowed by the access list, together with the router identified by the type and number, constitute the RP and its range of addresses for which it is responsible.

Use this command only in backbone routers that have good connectivity to all parts of the PIM domain. That is, a stub router that relies on an on-demand dialup link to connect to the rest of the PIM domain is not a good candidate RP.

When the **interval** keyword is specified, the candidate RP advertisement interval is set to a value specified by the *seconds* argument. The default interval is 60 seconds. Reducing this interval to a time of less than 60 seconds can reduce the time required to fail over to a secondary RP at the expense of generating more PIM Version 2 messages.

## Examples

The following example shows how to configure the router to advertise itself as a candidate RP to the BSR in its PIM domain. Standard access list number 4 specifies the group prefix associated with the RP that has the address identified by Ethernet interface 2. That RP is responsible for the groups with the prefix 239.

```
ip pim rp-candidate ethernet 2 group-list 4
access-list 4 permit 239.0.0.0 0.255.255.255
```

## Related Commands

| Command                        | Description                                                                    |
|--------------------------------|--------------------------------------------------------------------------------|
| <b>ip pim bsr-candidate</b>    | Configures the router to announce its candidacy as a BSR.                      |
| <b>ip pim rp-address</b>       | Configures the address of a PIM RP for a particular group.                     |
| <b>ip pim send-rp-announce</b> | Uses Auto-RP to configure for which groups the router is willing to act as RP. |

# ip pim send-rp-announce

To use Auto-RP to configure groups for which the router acts as a rendezvous point (RP), use the **ip pim send-rp-announce** command in global configuration mode. To unconfigure this router as an RP, use the **no** form of this command.

**ip pim** [**vrf** *vrf-name*] **send-rp-announce** *interface-type interface-number* **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*]

**no ip pim** [**vrf** *vrf-name*] **send-rp-announce** *interface-type interface-number*

| Syntax Description                               |  |                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vrf</b>                                       |  | (Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.                                                                                                                                                                                                            |
| <i>vrf-name</i>                                  |  | (Optional) Name assigned to the VRF.                                                                                                                                                                                                                                                                              |
| <i>interface-type</i><br><i>interface-number</i> |  | Interface type and number that is used to define the RP address. No space is required between the values.                                                                                                                                                                                                         |
| <b>scope</b> <i>ttl-value</i>                    |  | Specifies the time-to-live (TTL) value that limits the number of Auto-RP announcements.                                                                                                                                                                                                                           |
| <b>group-list</b> <i>access-list</i>             |  | (Optional) Specifies the standard IP access list number or name that defines the group prefixes that are advertised in association with the RP address. The access list name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid confusion with numbered access lists. |
| <b>interval</b> <i>seconds</i>                   |  | (Optional) Specifies the interval between RP announcements in seconds. The total holdtime of the RP announcements is automatically set to three times the value of the interval. The default interval is 60 seconds.                                                                                              |

**Command Default**

Auto-RP is disabled.  
*seconds*: 60

**Command Modes**

Global configuration

| Command History | Release   | Modification                                                                                                                                                                      |
|-----------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 11.1      | This command was introduced.                                                                                                                                                      |
|                 | 12.1(2)T  | This command was modified. The following keywords and argument were added: <ul style="list-style-type: none"> <li><b>interval</b> <i>seconds</i></li> <li><b>bidir</b></li> </ul> |
|                 | 12.0(23)S | This command was modified. The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.                                                                                        |
|                 | 12.2(13)T | This command was modified. The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.                                                                                        |

| Release     | Modification                                                                                                                                              |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(14)S   | This command was integrated into Cisco IOS Release 12.2(14)S.                                                                                             |
| 12.4(5)     | This command was modified. The <i>ip-address</i> argument was added.                                                                                      |
| 12.3(17)    | This command was modified. The <i>ip-address</i> argument was added.                                                                                      |
| 12.2(18)SXE | Support for this command was introduced on the Supervisor Engine 720.                                                                                     |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC.                                                                                           |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                           |
| 12.2(33)SRE | This command was modified. The <i>ip-address</i> argument was added.                                                                                      |
| 12.2(33)MRB | This command was integrated into Cisco IOS Release 12.2(33)MRB. This release does not support the <i>ip-address</i> argument or the <b>bidir</b> keyword. |

### Usage Guidelines

Enter this command on the router that you want to be an RP. When you are using Auto-RP to distribute group-to-RP mappings, this command causes the router to send an Auto-RP announcement message to the well-known group CISCO-RP-ANNOUNCE (224.0.1.39). This message announces the router as a candidate RP for the groups in the range described by the access list.

### Examples

The following example shows how to configure the router to send RP announcements out all Protocol Independent Multicast (PIM)-enabled interfaces for a maximum of 31 hops. The IP address by which the router wants to be identified as RP is the IP address associated with Ethernet interface 0. Access list 5 describes the groups for which this router serves as RP.

```
ip pim send-rp-announce ethernet0 scope 31 group-list 5
access-list 5 permit 224.0.0.0 15.255.255.255
```

### Related Commands

| Command                    | Description                                                                           |
|----------------------------|---------------------------------------------------------------------------------------|
| <b>ip pim rp-address</b>   | Configures the address of a PIM RP for a particular group.                            |
| <b>ip pim rp-candidate</b> | Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR. |

# ip pim send-rp-discovery

To configure the router to be a rendezvous point (RP) mapping agent, use the **ip pim send-rp-discovery** command in global configuration mode. To deconfigure the router from functioning as the RP mapping agent, use the **no** form of this command.

**ip pim** [**vrf** *vrf-name*] **send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value*

**no ip pim** [**vrf** *vrf-name*] **send-rp-discovery**

## Syntax Description

|                                                  |                                                                                                                                                              |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vrf</b> <i>vrf-name</i>                       | (Optional) Configures the router to be an RP mapping agent for the specified Multicast Virtual Private Network (VPN) routing and forwarding (MVRP) instance. |
| <i>interface-type</i><br><i>interface-number</i> | (Optional) Interface type and number that is to be used as the source address of the RP mapping agent.                                                       |
| <b>scope</b> <i>ttl-value</i>                    | Specifies the time-to-live (TTL) value for Auto-RP discovery messages. The range is from 1 to 255.                                                           |

## Command Default

The router is not configured to be an RP mapping agent.

## Command Modes

Global configuration

## Command History

| Release       | Modification                                                                                                               |
|---------------|----------------------------------------------------------------------------------------------------------------------------|
| 11.1          | This command was introduced.                                                                                               |
| 12.0(23)S     | The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.                                                            |
| 12.2(13)T     | The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.                                                            |
| 12.2(14)S     | This command was integrated into Cisco IOS Release 12.2(14)S.                                                              |
| 12.2(18)SXE   | Support for this command was introduced on the Supervisor Engine 720.                                                      |
| 12.2(27)SBC   | This command was integrated into Cisco IOS Release 12.2(27)SBC.                                                            |
| 12.2(33)SRA   | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                            |
| 12.4(8)       | The <b>interval</b> keyword and <i>seconds</i> argument were added.                                                        |
| 12.4(9)T      | The <b>interval</b> keyword and <i>seconds</i> argument were added.                                                        |
| 12.2(33)SRB   | The <b>interval</b> keyword and <i>seconds</i> argument were added.                                                        |
| 12.2(18)SXF11 | The <b>interval</b> keyword and <i>seconds</i> argument were added.                                                        |
| 12.2(33)MRB   | This command was integrated into Cisco IOS Release 12.2(33)MRB. This release does not support the <b>interval</b> keyword. |

**Usage Guidelines**

Use the **ip pim send-rp-discovery** command to configure the router to be an RP mapping agent. An RP mapping agent receives Auto-RP announcement messages, which it stores in its local group-to-RP mapping cache. The RP mapping agent uses the information contained in the Auto-RP announcement messages to elect the RP. The RP mapping agent elects the candidate RP with the highest IP address as the RP for a group range.

The required **scope** keyword and *ttl-value* argument are used to specify the TTL value in the IP header of Auto-RP discovery messages.

**Note**

For the **scope** keyword and *ttl-value* argument, specify a TTL large enough to cover your Protocol Independent Multicast (PIM) domain.

When Auto-RP is used, the following events occur:

1. The RP mapping agent listens for Auto-RP announcement messages sent by candidate RPs to the well-known group address CISCO-RP-ANNOUNCE (224.0.1.39).
2. The RP mapping agents stores the information learned from Auto-RP announcement messages in its local group-to-RP mapping cache.
3. The RP mapping agents elects the candidate RP with the highest IP address as the RP and announces the RP in the Auto-RP discovery messages that it sends out.
4. The Auto-RP discovery messages that the RP mapping agent sends to the well-known group CISCO-RP-DISCOVERY (224.0.1.40), which Cisco routers join by default, contains the elected RP learned from the RP mapping agent's group-to-RP mapping cache.
5. PIM designated routers listen for the Auto-RP discovery messages sent to 224.0.1.40 to learn the RP and store the information about the RP in their local group-to-RP mapping caches.

Use the **show ip pim rp** command with the **mapping** keyword to display all the group-to-RP mappings that the router has learned from Auto-RP.

**Examples**

The following example shows how to configure a router to be an RP mapping agent. In this example, the RP mapping agent is configured to use loopback 0 as the source address for Auto-RP messages. The Auto-RP discovery messages sent by the RP mapping agent are configured to be sent out with a TTL of 20 hops.

```
ip pim send-rp-discovery loopback 0 scope 20
```

**Related Commands**

| Command               | Description                                                                    |
|-----------------------|--------------------------------------------------------------------------------|
| <b>show ip pim rp</b> | Displays active RPs that are cached with associated multicast routing entries. |

# ip pim ssm

To define the Source Specific Multicast (SSM) range of IP multicast addresses, use the **ip pim ssm** command in global configuration mode. To disable the SSM range, use the **no** form of this command.

**ip pim** [**vrf** *vrf-name*] **ssm** {**default** | **range** *access-list*}

**no ip pim** [**vrf** *vrf-name*] **ssm** {**default** | **range** *access-list*}

| Syntax Description              |                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>vrf</b>                      | (Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance. |
| <i>vrf-name</i>                 | (Optional) Name assigned to the VRF.                                                                   |
| <b>default</b>                  | Defines the SSM range access list to 232/8.                                                            |
| <b>range</b> <i>access-list</i> | Specifies the standard IP access list number or name defining the SSM range.                           |

**Command Default** The command is disabled.

**Command Modes** Global configuration

| Command History | Release     | Modification                                                          |
|-----------------|-------------|-----------------------------------------------------------------------|
|                 | 12.1(3)T    | This command was introduced.                                          |
|                 | 12.0(23)S   | The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.       |
|                 | 12.2(13)T   | The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.       |
|                 | 12.2(14)S   | This command was integrated into Cisco IOS Release 12.2(14)S.         |
|                 | 12.2(18)SXE | Support for this command was introduced on the Supervisor Engine 720. |
|                 | 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC.       |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.       |
|                 | 12.2(33)MRB | This command was integrated into Cisco IOS Release 12.2(33)MRB.       |

**Usage Guidelines** When an SSM range of IP multicast addresses is defined by the **ip pim ssm** command, no Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages are accepted or originated in the SSM range.

**Examples** The following example shows how to configure SSM service for the IP address range defined by access list 4:

```
access-list 4 permit 224.2.151.141
ip pim ssm range 4
```

| Related Commands | Command        | Description                                                                    |
|------------------|----------------|--------------------------------------------------------------------------------|
|                  | show ip pim rp | Displays active RPs that are cached with associated multicast routing entries. |



# ip pim version

To configure the Protocol Independent Multicast (PIM) version of the interface, use the **ip pim version** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**ip pim version** [1 | 2]

**no ip pim version**

|                    |   |                                      |
|--------------------|---|--------------------------------------|
| Syntax Description | 1 | (Optional) Configures PIM Version 1. |
|                    | 2 | (Optional) Configures PIM Version 2. |

|                 |           |
|-----------------|-----------|
| Command Default | Version 2 |
|-----------------|-----------|

|               |                         |
|---------------|-------------------------|
| Command Modes | Interface configuration |
|---------------|-------------------------|

| Command History | Release     | Modification                                                                                                                                                                      |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 11.3 T      | This command was introduced.                                                                                                                                                      |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                 | 12.2(33)MRB | This command was integrated into Cisco IOS Release 12.2(33)MRB.                                                                                                                   |

|                  |                                                                                                                                                                                                                                                      |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usage Guidelines | An interface in Version 2 mode automatically downgrades to Version 1 mode if that interface has a PIM Version 1 neighbor. The interface returns to Version 2 mode after all Version 1 neighbors disappear (that is, they are shut down or upgraded). |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|          |                                                                                  |
|----------|----------------------------------------------------------------------------------|
| Examples | The following example configures the interface to operate in PIM Version 1 mode: |
|----------|----------------------------------------------------------------------------------|

```
interface ethernet 0
 ip address 10.0.0.0 255.0.0.0
 ip pim sparse-dense-mode
 ip pim version 1
```

# keepalive

To enable keepalive packets and to specify the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface or before bringing the tunnel protocol down for a specific interface, use the **keepalive** command in interface configuration mode.

When the keepalive function is enabled, a keepalive packet is sent at the specified time interval to keep the interface active. To turn off keepalive packets entirely, use the **no** form of this command.

**keepalive** [*period* [*retries*]]

**no keepalive** [*period* [*retries*]]

## Syntax Description

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>period</i>  | (Optional) Integer value in seconds, that represents the time interval between messages sent by the Cisco IOS software to ensure that a network interface is alive. The value must be greater than 0, and the default is 10.                                                                                                                                                                                                                                                                                                                              |
| <i>retries</i> | (Optional) Number of times that the device continues to send keepalive packets without response before bringing the interface down. The integer value is greater than 1 and less than 255. If omitted, the value that was previously set is used; if no value was specified previously, the default value of 5 is used.<br><br>If this command is used with a tunnel interface, then this variable specifies the number of times that the device continues to send keepalive packets without response before bringing the tunnel interface protocol down. |

## Command Default

*period*: 10 seconds

*retries*: 5

If you enter the **keepalive** command with no arguments, the defaults for both arguments are used.

If you enter the **keepalive** command and the timeout (*period*) argument, the default number of retries (5) is used.

If you enter the **no keepalive** command, keepalive packets are disabled on the interface.

## Command Modes

Interface configuration

## Command History

| Release     | Modification                                                            |
|-------------|-------------------------------------------------------------------------|
| 10.0        | This command was introduced.                                            |
| 12.2(8)T    | The retries argument was added and made available on tunnel interfaces. |
| 12.2(13)T   | The default value for the retries argument was increased to 5.          |
| 12.2(14)S   | This command was integrated into Cisco IOS release 12.2(14)S.           |
| 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.          |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.         |

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2.                                                                                                                   |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

## Usage Guidelines

### Keepalive Time Interval

You can configure the keepalive time interval, which is the frequency at which the Cisco IOS software sends messages to itself (Ethernet and Token Ring) or to the other end (serial and tunnel), to ensure that a network interface is alive. The interval is adjustable in 1-second increments, down to a minimum of 1 second. An interface is declared down after three update intervals have passed without receiving a keepalive packet unless the retry value is set higher.

Setting the keepalive timer to a low value is useful for quickly detecting Ethernet interface failures (such as a transceiver cable disconnecting, or cable that is not terminated).

### Line Failure

A typical serial line failure involves losing the Carrier Detect (CD) signal. Because this sort of failure is typically noticed within a few milliseconds, adjusting the keepalive timer for quicker routing recovery is generally not useful.

### Keepalive Packets with Tunnel Interfaces

GRE keepalive packets may be sent either from both sides of a tunnel or from just one side. If they are sent from both sides, the *period* and *retries* arguments can be different at each side of the link. If you configure keepalives on only one side of the tunnel, the tunnel interface on the sending side might perceive the tunnel interface on the receiving side to be down because the sending interface is not receiving keepalives. From the receiving side of the tunnel, the link appears normal because no keepalives were enabled on the second side of the link.

### Dropped Packets

Because keepalive packets are treated as ordinary packets, it is possible that they can be dropped. To reduce the possibility of dropped keepalive packets causing the tunnel interface to be taken down, increase the number of retries.



#### Note

When adjusting the keepalive timer for a very-low-bandwidth serial interface, large datagrams can delay the smaller keepalive packets long enough to cause the line protocol to go down. You may need to experiment to determine the best values to use for the timeout and the number of retry attempts.

## Examples

The following example shows how to set the keepalive interval to 3 seconds:

```
Router(config)# interface ethernet 0
Router(config-if)# keepalive 3
```

The following example shows how to set the keepalive interval to 3 seconds and the retry value to 7:

```
Router(config)# interface tunnel 1
Router(config-if)# keepalive 3 7
```

# load-interval

To change the length of time for which data is used to compute load statistics, use the **load-interval** interface configuration command. Use the **no** form of this command to revert to the default setting.

**load-interval** *seconds*

**no load-interval** *seconds*

|                           |                |                                                                                                                                                             |
|---------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>seconds</i> | Length of time for which data is used to compute load statistics. Specify a value that is a multiple of 30, from 30 to 600 (30, 60, 90, 120, and so forth). |
|---------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                        |                          |
|------------------------|--------------------------|
| <b>Command Default</b> | 300 seconds (5 minutes). |
|------------------------|--------------------------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | Interface configuration |
|----------------------|-------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                     |
|------------------------|----------------|-------------------------------------------------------------------------|
|                        | 10.3           | This command was introduced.                                            |
|                        | 12.2(4)T       | This command was made available in Frame Relay DLCI configuration mode. |
|                        | 12.2(18)SXF    | Support for this command was introduced on the Supervisor Engine 720.   |
|                        | 12.2(28)SB     | This command was integrated into Cisco IOS Release 12.2(28)SB.          |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.         |
|                        | 12.4(19)MR2    | This command was integrated into Cisco IOS Release 12.4(19)MR2.         |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA.         |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | If you want load computations to be more reactive to short bursts of traffic, rather than averaged over 5-minute periods, you can shorten the length of time over which load averages are computed.                                                                                                                                                                                                    |
|                         | If the load interval is set to 30 seconds, new data is used for load calculations over a 30-second period. This data is used to compute load statistics, including input rate in bits and packets per second, output rate in bits and packets per second, load, and reliability.                                                                                                                       |
|                         | Load data is gathered every 5 seconds. This data is used for a weighted average calculation in which more-recent load data has more weight in the computation than older load data. If the load interval is set to 30 seconds, the average is computed for the last 30 seconds of load data.                                                                                                           |
|                         | The <b>load-interval</b> command allows you to change the default interval of 5 minutes to a shorter or longer period of time. If you change it to a shorter period of time, the input and output statistics displayed when you use the <b>show interface</b> command are more current, and based on more instantaneous data, rather than reflecting a more average load over a longer period of time. |
|                         | This command is often used for dial backup purposes, to increase or decrease the likelihood of a backup interface being implemented, but it can be used on any interface.                                                                                                                                                                                                                              |

---

**Examples**

In the following example, the default 5-minute average is set to a 30-second average. A burst in traffic that would not trigger a dial backup for an interface configured with the default 5-minute interval might trigger a dial backup for this interface that is set for a shorter, 30-second interval.

```
Router(config)# interface serial 0
Router(config-if)# load-interval 30
```

---

**Related Commands**

| Command                | Description               |
|------------------------|---------------------------|
| <b>show interfaces</b> | Displays ALC information. |

# match any

To configure the match criteria for a class map to be successful match criteria for all packets, use the **match any** command in class-map configuration mode. To remove all criteria as successful match criteria, use the **no** form of this command.

**match any**

**no match any**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No match criteria are specified.

**Command Modes** Class-map configuration

## Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(5)XE   | This command was introduced.                                                                                                                                                      |
| 12.0(5)T    | This command was integrated into Cisco IOS Release 12.0(5)T.                                                                                                                      |
| 12.1(1)E    | This command was integrated into Cisco IOS Release 12.1(1)E.                                                                                                                      |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2(31)SB  | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router.                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

## Examples

In the following configuration, all packets leaving Ethernet interface 0/1 are policed based on the parameters specified in policy-map class configuration mode:

```
Router(config)# class-map matchany
Router(config-cmap)# match any
Router(config-cmap)# exit

Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit

Router(config)# interface gigabitethernet0/1
Router(config-if)# service-policy output policy1
```

| Related Commands | Command                      | Description                                                                           |
|------------------|------------------------------|---------------------------------------------------------------------------------------|
|                  | <b>class-map</b>             | Creates a class map to be used for matching packets to a specified class.             |
|                  | <b>match input-interface</b> | Configures a class map to use the specified input interface as a match criterion.     |
|                  | <b>match protocol</b>        | Configures the match criteria for a class map on the basis of the specified protocol. |

# match atm clp

To enable packet matching on the basis of the ATM cell loss priority (CLP), use the **match atm clp** command in class-map configuration mode. To disable packet matching on the basis of the ATM CLP, use the **no** form of this command.

**match atm clp**

**no match atm clp**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Packets are not matched on the basis of the ATM CLP.

## Command Modes

Class-map configuration (config-cmap)

## Command History

| Release                  | Modification                                                                                                                                        |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(28)S                | This command was introduced.                                                                                                                        |
| 12.2(28)SB               | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                                      |
| 12.2(33)SRB              | This command was integrated into Cisco IOS Release 12.2(33)SRB.                                                                                     |
| 12.2(33)SRC              | Support for the Cisco 7600 series router was added.                                                                                                 |
| 12.4(15)T2               | This command was integrated into Cisco IOS Release 12.4(15)T2.                                                                                      |
| 12.2(33)SB               | Support for the Cisco 7300 series router was added.                                                                                                 |
| Cisco IOS XE Release 2.3 | This command was integrated into Cisco IOS XE Release 2.3.                                                                                          |
| 12.4(20)MR               | This command was integrated into Cisco IOS Release 12.4(20)MR. This release uses the syntax <b>match atm clp</b> instead of <b>match atm-clp</b> .  |
| 12.2(33)MRA              | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release uses the syntax <b>match atm clp</b> instead of <b>match atm-clp</b> . |

## Usage Guidelines

This command is supported on policy maps that are attached to ATM main interfaces, ATM subinterfaces, or ATM permanent virtual circuits (PVCs). However, policy maps (containing the **match atm clp** command) that are attached to these types of ATM interfaces can be *input* policy maps *only*.

This command is supported on the PA-A3 adapter *only*.



## Examples

In the following example, a class called “class-c1” has been created using the **class-map** command, and the **match atm clp** command has been configured inside that class. Therefore, packets are matched on the basis of the ATM CLP and are placed into this class.

```
Router> enable
Router# configure terminal
Router(config)# class-map class-c1
Router(config-cmap)# match atm clp
Router(config-cmap)# end
```

## Related Commands

| Command                          | Description                                                                                                                                                                         |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>class-map</b>                 | Creates a class map to be used for matching packets to a specified class.                                                                                                           |
| <b>show atm pvc</b>              | Displays all ATM PVCs and traffic information.                                                                                                                                      |
| <b>show policy-map interface</b> | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# match cos

To match a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking, use the **match cos** command in class-map configuration mode. To remove a specific Layer 2 CoS/ISL marking as a match criterion, use the **no** form of this command.

**match cos** *cos-value* [*cos-value* [*cos-value* [*cos-value*]]]

**no match cos** *cos-value* [*cos-value* [*cos-value* [*cos-value*]]]

|                           |                  |                                                                                                                                                                           |
|---------------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>cos-value</i> | Specific IEEE 802.1Q/ISL CoS value. The <i>cos-value</i> is from 0 to 7; up to four CoS values, separated by a space, can be specified in one <b>match cos</b> statement. |
|---------------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                        |                                                                    |
|------------------------|--------------------------------------------------------------------|
| <b>Command Default</b> | Packets are not matched on the basis of a Layer 2 CoS/ISL marking. |
|------------------------|--------------------------------------------------------------------|

|                      |                                       |
|----------------------|---------------------------------------|
| <b>Command Modes</b> | Class-map configuration (config-cmap) |
|----------------------|---------------------------------------|

| Command History | Release     | Modification                                                                                                                                                                      |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.1(5)T    | This command was introduced.                                                                                                                                                      |
|                 | 12.0(25)S   | This command was integrated into Cisco IOS Release 12.0(25)S.                                                                                                                     |
|                 | 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                                                                    |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2(31)SB  | This command was implemented on the Cisco 10000 series router.                                                                                                                    |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                 | 12.2(33)SRC | Support for the Cisco 7600 series router was added.                                                                                                                               |
|                 | 12.4(15)T2  | This command was integrated into Cisco IOS Release 12.4(15)T2.                                                                                                                    |
|                 | 12.2(33)SB  | Support for the Cisco 7300 series router was added.                                                                                                                               |
|                 | 12.4(20)MR  | This command was incorporated into Cisco IOS Release 12.4(20)MR.                                                                                                                  |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

|                 |                                                                                                                                                             |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | In the following example, the CoS values of 1, 2, and 3 are successful match criteria for the interface that contains the classification policy called cos: |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
Router(config)# class-map cos
Router(config-cmap)# match cos 1 2 3
```

In the following example, classes called voice and video-n-data are created to classify traffic based on the CoS values. QoS treatment is then given to the appropriate packets in the CoS-based-treatment policy map (in this case, the QoS treatment is priority 64 and bandwidth 512). The service policy configured in this example is attached to all packets leaving Fast Ethernet interface 0/0.1. The service policy can be attached to any interface that supports service policies.

```
Router(config)# class-map voice
Router(config-cmap)# match cos 7

Router(config)# class-map video-n-data
Router(config-cmap)# match cos 5

Router(config)# policy-map cos-based-treatment
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 64
Router(config-pmap-c)# exit
Router(config-pmap)# class video-n-data
Router(config-pmap-c)# bandwidth 512
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# interface fastethernet0/0.1
Router(config-if)# service-policy output cos-based-treatment
```

#### Related Commands

| Command               | Description                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>class-map</b>      | Creates a class map to be used for matching packets to a specified class.                                                                   |
| <b>policy-map</b>     | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                |
| <b>service-policy</b> | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| <b>set cos</b>        | Sets the Layer 2 CoS value of an outgoing packet.                                                                                           |
| <b>show class-map</b> | Displays all class maps and their matching criteria.                                                                                        |

# match dscp

To identify one or more differentiated service code point (DSCP), Assured Forwarding (AF), and Certificate Server (CS) values as a match criterion, use the **match dscp** command in class-map configuration mode. To remove a specific DSCP value from a class map, use the **no** form of this command.

```
match [ip] dscp dscp-value [dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value]
```

```
no match [ip] dscp dscp-value
```

|                    |            |                                                                                                                        |
|--------------------|------------|------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | ip         | (Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets. |
|                    | dscp-value | The DSCP value used to identify a DSCP value. For valid values, see the Usage Guidelines.                              |

|                 |                                                                                                                               |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------|
| Command Default | No match criteria is configured.<br>If you do not enter the <b>ip</b> keyword, matching occurs on both IPv4 and IPv6 packets. |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------|

|               |                         |
|---------------|-------------------------|
| Command Modes | Class-map configuration |
|---------------|-------------------------|

|                 |             |                                                                                      |
|-----------------|-------------|--------------------------------------------------------------------------------------|
| Command History | Release     | Modification                                                                         |
|                 | 12.2(13)T   | This command was introduced. This command replaces the <b>match ip dscp</b> command. |
|                 | 12.0(28)S   | Support for this command in IPv6 was added in Cisco IOS Release S12.0(28)S on the    |
|                 | 12.0(17)SL  | This command was implemented on the Cisco 10000 series router.                       |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                       |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                      |

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usage Guidelines | <b>DSCP Values</b><br>You must enter one or more differentiated service code point (DSCP) values. The command may include any combination of the following: <ul style="list-style-type: none"><li>• numbers (0 to 63) representing differentiated services code point values</li><li>• af numbers (for example, af11) identifying specific AF DSCPs</li><li>• cs numbers (for example, cs1) identifying specific CS DSCPs</li><li>• <b>default</b>—Matches packets with the default DSCP.</li><li>• <b>ef</b>—Matches packets with EF DSCP.</li></ul> |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

For example, if you wanted the DSCP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified DSCP values), enter the **match dscp 0 1 2 3 4 5 6 7** command.

This command is used by the class map to identify a specific DSCP value marking on a packet. In this context, *dscp-value* arguments are used as markings only and have no mathematical significance. For instance, the *dscp-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *dscp-value* of 2 is different than a packet marked with the *dscp-value* of 1. The treatment of these marked packets is defined by the user through the setting of Quality of Service (QoS) policies in policy-map class configuration mode.

### Match Packets on DSCP Values

To match DSCP values for IPv6 packets only, the **match protocol ipv6** command must also be used. Without that command, the DSCP match defaults to match both IPv4 and IPv6 packets.

To match DSCP values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword the match occurs on both IPv4 and IPv6 packets. Alternatively, the **match protocol ip** command may be used with **match dscp** to classify only IPv4 packets.

After the DSCP bit is set, other QoS features can then operate on the bit settings.

The network can give priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data is then queued according to the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) can ensure that high-precedence traffic has lower loss rates than other traffic during times of congestion.

### Examples

The following example shows how to set multiple match criteria. In this case, two IP DSCP value and one AF value.

```
Router(config)# class-map map1
Router(config-cmap)# match dscp 1 2 af11
```

### Related Commands

| Command                  | Description                                                                                                                                 |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>class-map</b>         | Creates a class map to be used for matching packets to a specified class.                                                                   |
| <b>match protocol ip</b> | Matches DSCP values for packets.                                                                                                            |
| <b>policy-map</b>        | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                |
| <b>service-policy</b>    | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| <b>set dscp</b>          | Marks the DSCP value for packets within a traffic class.                                                                                    |
| <b>show class-map</b>    | Displays all class maps and their matching criteria.                                                                                        |

# match ip dscp

To identify a specific IP differentiated service code point (DSCP) value as a match criterion, use the **match ip dscp** class-map configuration command. To remove a specific IP DSCP value from a class map, use the **no** form of this command.

**match ip dscp** *ip-dscp-value* [*ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value*]

**no match ip dscp** *ip-dscp-value* [*ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value*]

## Syntax Description

*ip-dscp-value* Specifies the exact value from 0 to 63 used to identify an IP DSCP value.

## Command Modes

Class-map configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

Up to eight IP DSCP values can be matched in one match statement. For example, if you wanted the IP DSCP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified IP DSCP values), enter the **match ip dscp 0 1 2 3 4 5 6 7** command.

This command is used by the class map to identify a specific IP DSCP value marking on a packet. The *ip-dscp-value* arguments are used as markings only. The IP DSCP values have no mathematical significance. For instance, the *ip-dscp-value* of 2 is not greater than 1. The value simply indicates that a packet marked with an *ip-dscp-value* of 2 is different from a packet marked with an *ip-dscp-value* of 1. The treatment of these marked packets is defined by the user through the setting of QoS policies in policy-map class configuration mode.

## Examples

The following example shows how to configure the service policy called priority55 and attach service policy priority55 to an interface. In this example, the class map called ipdscp15 evaluates all packets entering interface Fast Ethernet 0/0 for an IP DSCP value of 15. If the incoming packet has been marked with the IP DSCP value of 15, the packet is treated with a priority level of 55.

```
Router(config)# class-map ipdscp15
Router(config-cmap)# match ip dscp 15
Router(config-cmap)# exit
Router(config)# policy-map priority55
Router(config-pmap)# class ipdscp15
Router(config-pmap-c)# priority55
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa0/0
Router(config-if)# service-policy input priority55
```

## Related Commands

| Command               | Description                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>class-map</b>      | Creates a class map to be used for matching packets to a specified class.                                                                   |
| <b>policy-map</b>     | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                |
| <b>service-policy</b> | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| <b>set ip dscp</b>    | Marks the IP DSCP value for packets within a traffic class.                                                                                 |
| <b>show class-map</b> | Displays all class maps and their matching criteria.                                                                                        |

# match mpls experimental

To configure a class map to use the specified value or values of the experimental (EXP) field as a match criteria, use the **match mpls experimental** command in class-map configuration mode. To remove the EXP field match criteria from a class map, use the **no** form of this command.

**match mpls experimental** *number*

**no match mpls experimental** *number*

|                           |               |                                                                                                                                                            |
|---------------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>number</i> | EXP field value (any number from 0 through 7) to be used as a match criterion. You can specify multiple values, separated by a space (for example, 3 4 7). |
|---------------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                        |                                  |
|------------------------|----------------------------------|
| <b>Command Default</b> | No match criteria are specified. |
|------------------------|----------------------------------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | Class-map configuration |
|----------------------|-------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                                                               |
|------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | 12.0(7)XE1     | This command was introduced.                                                                                                                                                      |
|                        | 12.1(1)E       | This command was integrated into Cisco IOS Release 12.1(1)E.                                                                                                                      |
|                        | 12.1(5)T       | This command was integrated into Cisco IOS Release 12.1(5)T.                                                                                                                      |
|                        | 12.2(4)T       | This command was implemented on the Cisco MGX 8850 switch and the MGX 8950 switch with a Cisco MGX RPM-PR card.                                                                   |
|                        | 12.2(4)T2      | This command was implemented on the Cisco 7500 series.                                                                                                                            |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                        | 12.2(31)SB     | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series.                                                                          |
|                        | 12.2SX         | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

|                         |                                                                                                                                                                                                                                                                                                                                     |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria such as input interfaces, access control lists (ACLs), protocols, quality of service (QoS) labels, and experimental (EXP) field values. Packets satisfying the match criteria for a class constitute the traffic for that class. |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

The **match mpls experimental** command specifies the name of an EXP field value to be used as the match criterion against which packets are compared to determine if they belong to the class specified by the class map.



To use the **match mpls experimental** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

For CBWFQ, you define traffic classes based on match criteria such as input interfaces, ACLs, protocols, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

To use the **match mpls experimental** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

## Examples

The following example specifies a class map called ethernet1 and configures the Multiprotocol Label Switching (MPLS) experimental values of 1 and 2 to be used as the match criteria for this class:

```
Router(config)# class-map ethernet1
Router(config-cmap)# match mpls experimental 1 2
```

## Related Commands

| Command                                | Description                                                                       |
|----------------------------------------|-----------------------------------------------------------------------------------|
| <b>class-map</b>                       | Creates a class map to be used for matching packets to a specified class.         |
| <b>match access-group</b>              | Configures the match criteria for a class map based on the specified ACL.         |
| <b>match input-interface</b>           | Configures a class map to use the specified input interface as a match criterion. |
| <b>match mpls experimental topmost</b> | Matches the EXP value in the topmost label.                                       |
| <b>match protocol</b>                  | Matches traffic by a particular protocol.                                         |
| <b>match qos-group</b>                 | Configures the match criteria for a class map based on the specified protocol.    |

# match precedence

To identify IP precedence values to use as the match criterion, use the **match precedence** command in class-map configuration mode. To remove IP precedence values from a class map, use the **no** form of this command.

**match [ip] precedence** {*precedence-criteria1* | *precedence-criteria2* | *precedence-criteria3* | *precedence-criteria4*}

**no match [ip] precedence** {*precedence-criteria1* | *precedence-criteria2* | *precedence-criteria3* | *precedence-criteria4*}

|                           |                             |                                                                                                                                                |
|---------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>ip</b>                   | (Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IP and IPv6 packets.                           |
|                           | <i>precedence-criteria1</i> | Identifies the precedence value. You can enter up to four different values, separated by a space. See the “Usage Guidelines” for valid values. |
|                           | <i>precedence-criteria2</i> |                                                                                                                                                |
|                           | <i>precedence-criteria3</i> |                                                                                                                                                |
|                           | <i>precedence-criteria4</i> |                                                                                                                                                |

|                        |                                                                                           |
|------------------------|-------------------------------------------------------------------------------------------|
| <b>Command Default</b> | No match criterion is configured.                                                         |
|                        | If you do not enter the <b>ip</b> keyword, matching occurs on both IPv4 and IPv6 packets. |

|                      |                                            |
|----------------------|--------------------------------------------|
| <b>Command Modes</b> | Class-map configuration mode (config-cmap) |
|----------------------|--------------------------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                        |
|------------------------|----------------|--------------------------------------------------------------------------------------------|
|                        | 12.2(13)T      | This command was introduced. This command replaces the <b>match ip precedence</b> command. |
|                        | 12.0(17)SL     | This command was implemented on the Cisco 10000 series router.                             |
|                        | 12.0(28)S      | Support for this command in IPv6 was added on the Cisco 12000 series Internet router.      |
|                        | 12.2(31)SB     | This command was integrated into Cisco IOS Release 12.2(31)SB.                             |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.                             |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA.                            |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | <p>You can enter up to four matching criteria, as number abbreviation (0 to 7) or criteria names (critical, flash, and so on), in a single match statement. For example, if you wanted the precedence values of 0, 1, 2, or 3 (note that only one of the precedence values must be a successful match criterion, not all of the specified precedence values), enter the <b>match ip precedence 0 1 2 3</b> command. The <i>precedence-criteria</i> numbers are not mathematically significant; that is, the <i>precedence-criteria</i> of 2 is not greater than 1. The way that these different packets are treated depends upon quality of service (QoS) policies, set in the policy-map configuration mode.</p> |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

You can configure a QoS policy to include IP precedence marking for packets entering the network. Devices within your network can then use the newly marked IP precedence values to determine how to treat the packets. For example, class-based weighted random early detection (WRED) uses IP precedence values to determine the probability that a packet is dropped. You can also mark voice packets with a particular precedence. You can then configure low-latency queueing (LLQ) to place all packets of that precedence into the priority queue.

### Precedence Values and Names

The following table lists all criteria conditions by value, name, binary value, and recommended use. You may enter up to four criteria, each separated by a space. Only one of the precedence values must be a successful match criterion. [Table 5](#) lists the IP precedence values.

**Table 5** *IP Precedence Values*

| Precedence Value | Precedence Name    | Binary Value | Recommended Use                                                            |
|------------------|--------------------|--------------|----------------------------------------------------------------------------|
| 0                | routine            | 000          | Default marking value                                                      |
| 1                | priority           | 001          | Data applications                                                          |
| 2                | immediate          | 010          | Data applications                                                          |
| 3                | flash              | 011          | Call signaling                                                             |
| 4                | flash-override     | 100          | Video conferencing and streaming video                                     |
| 5                | critical           | 101          | Voice                                                                      |
| 6                | internet (control) | 110          | Network control traffic (such as routing, which is typically precedence 6) |
| 7                | network (control)  | 111          |                                                                            |

Do not use IP precedence 6 or 7 to mark packets, unless you are marking control packets.

## Examples

### IPv4-Specific Traffic Match

The following example shows how to configure the service policy called “priority50” and attach service policy “priority50” to an interface, matching for IPv4 traffic only. In a network where both IPv4 and IPv6 are running, you might find it necessary to distinguish between the protocols for matching and traffic segregation. In this example, the class map called “ipprec5” evaluates all IPv4 packets entering Fast Ethernet interface 1/0/0 for a precedence value of 5. If the incoming IPv4 packet has been marked with the precedence value of 5, the packet is treated as priority traffic and is allocated bandwidth of 50 kbps.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match ip precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

### IPv6-Specific Traffic Match

The following example shows the same service policy matching on precedence for IPv6 traffic only. Notice that the **match protocol** command with the **ipv6** keyword precedes the **match precedence** command. The **match protocol** command is required to perform matches on IPv6 traffic alone.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match protocol ipv6
Router(config-cmap)# match precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

### Related Commands

| Command                  | Description                                                                                                                                 |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>class-map</b>         | Creates a class map to be used for matching packets to a specified class.                                                                   |
| <b>match protocol</b>    | Configures the match criteria for a class map on the basis of a specified protocol.                                                         |
| <b>policy-map</b>        | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                |
| <b>service-policy</b>    | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| <b>set ip precedence</b> | Sets the precedence value in the IP header.                                                                                                 |
| <b>show class-map</b>    | Displays all class maps and their matching criteria, or a specified class map and its matching criteria.                                    |

# match qos-group

To identify a specific quality of service (QoS) group value as a match criterion, use the **match qos-group** command in class-map configuration mode. To remove a specific QoS group value from a class map, use the **no** form of this command.

**match qos-group** *qos-group-value*

**no match qos-group** *qos-group-value*

## Syntax Description

|                        |                                                                  |
|------------------------|------------------------------------------------------------------|
| <i>qos-group-value</i> | The exact value from 0 to 99 used to identify a QoS group value. |
|------------------------|------------------------------------------------------------------|

## Command Default

No match criterion is specified.

## Command Modes

Class-map configuration (config-cmap)

## Command History

| Release                  | Modification                                                                                                                                                                      |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.1CC                   | This command was introduced.                                                                                                                                                      |
| 12.05(XE)                | This command was integrated into Cisco IOS Release 12.0(5)XE.                                                                                                                     |
| 12.2(13)T                | This command was integrated into Cisco IOS Release 12.2(13)T.                                                                                                                     |
| 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2(31)SB               | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series.                                                                          |
| 12.2SX                   | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers.                                                                                                                    |
| 12.4(20)MR               | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA              | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

## Usage Guidelines

The **match qos-group** command is used by the class map to identify a specific QoS group value marking on a packet. This command can also be used to convey the received Multiprotocol Label Switching (MPLS) experimental (EXP) field value to the output interface.

The *qos-group-value* argument is used as a marking only. The QoS group values have no mathematical significance. For instance, the *qos-group-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *qos-group-value* of 2 is different than a packet marked with the *qos-group-value* of 1. The treatment of these packets is defined by the user through the setting of QoS policies in QoS policy-map class configuration mode.

The QoS group value is local to the router, meaning that the QoS group value that is marked on a packet does not leave the router when the packet leaves the router. If you need a marking that resides in the packet, use IP precedence setting, IP differentiated services code point (DSCP) setting, or another method of packet marking.

This command can be used with the **random-detect discard-class-based** command.

## Examples

The following example shows how to configure the service policy called *priority50* and attach service policy *priority50* to an interface. In this example, the class map called *qosgroup5* evaluates all packets entering GigabitEthernet interface 1/0/0 for a QoS group value of 5. If the incoming packet has been marked with the QoS group value of 5, the packet is treated with a priority level of 50.

```
Router(config)# class-map qosgroup5
Router(config-cmap)# match qos-group 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class qosgroup5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet1/0/0
Router(config-if)# service-policy output priority50
```

## Related Commands

| Command                                  | Description                                                                                                                                 |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>class-map</b>                         | Creates a class map to be used for matching packets to a specified class.                                                                   |
| <b>policy-map</b>                        | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                |
| <b>random-detect discard-class-based</b> | Bases WRED on the discard class value of a packet.                                                                                          |
| <b>service-policy</b>                    | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| <b>set precedence</b>                    | Specifies an IP precedence value for packets within a traffic class.                                                                        |
| <b>set qos-group</b>                     | Sets a group ID that can be used later to classify packets.                                                                                 |

# match vlan (QoS)

To match and classify traffic on the basis of the VLAN identification number, use the **match vlan** command in class-map configuration mode. To remove a previously specified VLAN identification number as a match criterion, use the **no** form of this command.

**match vlan** *vlan-id-number*

**no match vlan** *vlan-id-number*

## Syntax Description

|                       |                                                                                                                                |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <i>vlan-id-number</i> | VLAN identification number, numbers, or range of numbers. Valid VLAN identification numbers must be in the range of 1 to 4095. |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------|

## Command Default

Traffic is not matched on the basis of the VLAN identification number.

## Command Modes

Class-map configuration

## Command History

| Release     | Modification                                                            |
|-------------|-------------------------------------------------------------------------|
| 12.2(31)SB2 | This command was introduced for use on Cisco 10000 series routers only. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.          |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.         |

## Usage Guidelines

### Specifying VLAN Identification Numbers

You can specify a single VLAN identification number, multiple VLAN identification numbers separated by spaces (for example, 2 5 7), or a range of VLAN identification numbers separated by a hyphen (for example, 25-35).

### Support Restrictions

The **match vlan** command is supported for IEEE 802.1q and Inter-Switch Link (ISL) VLAN encapsulations only.

## Examples

In the following sample configuration, the **match vlan** command is enabled to classify and match traffic on the basis of a range of VLAN identification numbers. Packets with VLAN identification numbers in the range of 25 to 50 are placed in the class called class1.

```
Router> enable
Router# configure terminal
Router(config)# class-map class1
Router(config-cmap)# match vlan 25-50
Router(config-cmap)# end
```

**Note**

Typically, the next step would be to configure class1 in a policy map, enable a quality of service (QoS) feature (for example, class-based weighted fair queueing [CBWFQ]) in the policy map, and attach the policy map to an interface. To configure a policy map, use the **policy-map** command. To enable CBWFQ, use the **bandwidth** command (or use the command for the QoS feature that you want to enable). To attach the policy map to an interface, use the **service-policy** command. For more information about classifying network traffic on the basis of a match criterion, see the Classification section of the *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2SR*.

**Related Commands**

| Command                                | Description                                                                        |
|----------------------------------------|------------------------------------------------------------------------------------|
| <b>bandwidth</b><br>(policy-map class) | Specify or modifies the bandwidth allocated for a class belonging to a policy map. |
| <b>class-map</b>                       | Creates a class map to be used for matching packets to a specified class.          |
| <b>policy-map</b>                      | Creates or modifies a policy map that can be attached to one or more interfaces.   |
| <b>service-policy</b>                  | Attached a policy map to an interface.                                             |



# maximum meps

To specify the number of maintenance endpoints (MEPs) across the network in a maintenance association, use the **maximum meps** command in Ethernet CFM service configuration mode. To restore the default value, use the **no** form of this command.

**maximum meps** *max-num*

**no maximum meps**

## Syntax Description

*max-num* Integer from 1 to 65535. The default is 100.

## Command Default

A maximum number of MEPs is not configured.

## Command Modes

Ethernet CFM service configuration (config-ecfm-srv)

## Command History

| Release      | Modification                                                    |
|--------------|-----------------------------------------------------------------|
| 12.2(33)SX12 | This command was introduced.                                    |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

When the configured maximum is reached, continuity check messages (CCMs) from other remote MEPs are ignored and a warning message is displayed.

Output of the **show running all** command displays “maximum meps 100” when the default value is configured.

## Examples

The following example shows how to configure a maximum of 50 MEPs:

```
Router(config)# ethernet cfm domain operatorA level 5
Router(config-ether-cfm)# service vlan-id 5 port
Router(config-ether-cfm)# maximum meps 50
```

## Related Commands

| Command                 | Description                                          |
|-------------------------|------------------------------------------------------|
| <b>show running all</b> | Shows the running configuration with default values. |

# mdt data

To configure the multicast group address range for data multicast distribution tree (MDT) groups, use the **mdt data** command in VRF configuration mode. To disable this function, use the **no** form of this command.

**mdt data** *group-address-range wildcard-bits* [**threshold** *threshold-value*] [**list** *access-list*]

**no mdt data** *group-address-range wildcard-bits* [**threshold** *threshold-value*] [**list** *access-list*]

## Syntax Description

|                                         |                                                                                        |
|-----------------------------------------|----------------------------------------------------------------------------------------|
| <i>group-address-range</i>              | Multicast group address range. The range is from 224.0.0.1 to 239.255.255.255.         |
| <i>wildcard-bits</i>                    | Wildcard bits to be applied to the multicast group address range.                      |
| <b>threshold</b> <i>threshold-value</i> | (Optional) Defines the bandwidth threshold value. The range is from 1 through 4294967. |
| <b>list</b> <i>access-list</i>          | (Optional) Defines the access list name or number.                                     |

## Command Default

The command is disabled.

## Command Modes

VRF configuration

## Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(23)S   | This command was introduced.                                                                                                                                                      |
| 12.2(13)T   | This command was integrated into Cisco IOS Release 12.2(13)T.                                                                                                                     |
| 12.2(14)S   | This command was integrated into Cisco IOS Release 12.2(14)S.                                                                                                                     |
| 12.2(18)SXE | Support for this command was introduced on the Supervisor Engine 720.                                                                                                             |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC.                                                                                                                   |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)MRB | This command was integrated into Cisco IOS Release 12.2(33)MRB.                                                                                                                   |

## Usage Guidelines

A data MDT group can include a maximum of 256 multicast groups per Virtual Private Network (VPN). Multicast groups used to create the data MDT group are dynamically chosen from a pool of configured IP addresses.

This command configures a range of alternative multicast destination addresses for the tunnel header. The destination address chosen depends on the traffic profile (that is, the source and destination match the specified access list and the rate of the traffic has exceeded the bandwidth threshold value).

## Examples

In the following example, Protocol Independent Multicast (PIM) Source Specific Multicast (SSM) is configured in the backbone. Therefore, the default and data MDT groups are configured within the SSM range of IP addresses. Inside the VPN, PIM sparse mode (PIM-SM) is configured and only Auto-RP announcements are accepted.

```
!
ip vrf vrf1
  rd 1:1
  route-target export 1:1
  route-target import 1:1
  mdt default 232.0.0.1
  mdt data 232.0.1.0 0.0.0.255 threshold 500 list 101
!
.
.
.
!
ip pim ssm default
ip pim vrf vrf1 accept-rp auto-rp
!
```

## Related Commands

| Command            | Description                                   |
|--------------------|-----------------------------------------------|
| <b>mdt default</b> | Configures a default MDT group for a VPN VRF. |

# mdt default

To configure a default multicast distribution tree (MDT) group for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **mdt default** command in VRF configuration mode. To disable this function, use the **no** form of this command.

**mdt default** *group-address*

**no mdt default** *group-address*

|                           |                      |                                                                                                                                                                                                                                                         |
|---------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>group-address</i> | IP address of the default MDT group. This address serves as an identifier for the community in that provider-edge (PE) routers configured with the same group address become members of the group, allowing them to receive packets sent by each other. |
|---------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                        |                          |
|------------------------|--------------------------|
| <b>Command Default</b> | The command is disabled. |
|------------------------|--------------------------|

|                      |                   |
|----------------------|-------------------|
| <b>Command Modes</b> | VRF configuration |
|----------------------|-------------------|

|                        |                |                                                                       |
|------------------------|----------------|-----------------------------------------------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                   |
|                        | 12.0(23)S      | This command was introduced.                                          |
|                        | 12.2(13)T      | This command was integrated into Cisco IOS Release 12.2(13)T.         |
|                        | 12.2(14)S      | This command was integrated into Cisco IOS Release 12.2(14)S.         |
|                        | 12.2(18)SXE    | Support for this command was introduced on the Supervisor Engine 720. |
|                        | 12.2(27)SBC    | This command was integrated into Cisco IOS Release 12.2(27)SBC.       |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.       |
|                        | 12.2(33)MRB    | This command was integrated into Cisco IOS Release 12.2(33)MRB.       |

|                         |                                                                                                                                                                                 |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | The default MDT group must be the same group configured on all PE routers that belong to the same VPN.                                                                          |
|                         | If Source Specific Multicast (SSM) is used as the protocol for the default MDT, the source IP address is the address used to source the Border Gateway Protocol (BGP) sessions. |
|                         | A tunnel interface is created as a result of this command. By default, the destination address of the tunnel header is the <i>group-address</i> argument.                       |

|                 |                                                                                                                                                                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | In the following example, Protocol Independent Multicast (PIM) SSM is configured in the backbone. Therefore, the default and data MDT groups are configured within the SSM range of IP addresses. Inside the VPN, PIM sparse mode (PIM-SM) is configured and only Auto-RP announcements are accepted. |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
!  
ip vrf vrf1  
  rd 1:1
```

```

route-target export 1:1
route-target import 1:1
mdt default 232.0.0.1
mdt data 232.0.1.0 0.0.0.255 threshold 500 list 101
!
.
!
ip pim ssm default
ip pim vrf vrf1 accept-rp auto-rp
!
```

#### Related Commands

| Command         | Description                                                       |
|-----------------|-------------------------------------------------------------------|
| <b>mdt data</b> | Configures the multicast group address range for data MDT groups. |

# mep archive-hold-time

To set the amount of time, in minutes, that data from a missing maintenance end point (MEP) is kept in the continuity check database or that entries are held in the error database before they are purged, use the **mep archive-hold-time** command in Ethernet connectivity fault management (CFM) configuration mode. To restore the default number of minutes, use the **no** form of this command.



## Note

Release 12.2(33)MRA supports the Draft 1.0 version of Ethernet CFM; it does not support the IEEE 802.1ag-2007 version.

**mep archive-hold-time** *minutes*

**no mep archive-hold-time** *minutes*

## Syntax Description

|                |                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <i>minutes</i> | Integer from 1 to 65535 that specifies the number of minutes that data from a missing MEP is kept before it is purged. The default is 100. |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|

## Command Default

The command is enabled, and the archive hold time is set to 100 minutes.

## Command Modes

### Cisco pre-Standard CFM Draft 1 (CFM D1)

Ethernet CFM configuration (config-ether-cfm)

### CFM IEEE 802.1ag Standard (CFM IEEE)

Ethernet CFM configuration (config-ether-cfm)

## Command History

| Release      | Modification                                                                                                                 |
|--------------|------------------------------------------------------------------------------------------------------------------------------|
| 12.2(33)SRA  | This command was introduced.                                                                                                 |
| 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T.                                                                |
| 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.                                                              |
| 12.2(33)SXI2 | This command was integrated into Cisco IOS Release 12.2(33)SXI2. In this release the command was supported only in CFM IEEE. |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                              |

## Usage Guidelines

When you reset the archive hold time, the new hold time applies only to entries in the database that occur after the reset. Entries made before the hold time was reset are not affected by the change.

Different archive hold times can be set for MEPs in different domains.



## Note

A missing MEP is a remote MEP that sends a 0 expiration time in its continuity check or a remote MEP whose entry in the local continuity check database expires after it exceeds its lifetime.

In CFM IEEE, output of the **show running all** command displays “mep archive hold-time 100” when the default value is configured.

### Examples

The following example shows how to set a timeout period of 1000 minutes in CFM D1:

```
Router(config-ether-cfm)# mep archive-hold-time 1000
```

The following example shows how to set a timeout period of 1000 minutes in CFM IEEE:

```
Router(config-ether-cfm)# mep archive-hold-time 1000
```

### Related Commands

| Command                 | Description                                          |
|-------------------------|------------------------------------------------------|
| <b>show running all</b> | Shows the running configuration with default values. |

# mep crosscheck mpid vlan

To statically define a remote maintenance endpoint (MEP) within a maintenance domain, use the **mep crosscheck mpid vlan** command in Ethernet CFM configuration mode. To delete a remote MEP, use the **no** form of this command.

**mep crosscheck mpid id vlan** *vlan-id* [**mac** *mac-address*]

**no mep crosscheck mpid id vlan** *vlan-id* [**mac** *mac-address*]

|                           |                    |                                                                               |
|---------------------------|--------------------|-------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>id</i>          | Integer in the range of 0 to 8191 that forms the maintenance point ID (MPID). |
|                           | <i>vlan-id</i>     | Integer in the range of 1 to 4094 that identifies the VLAN.                   |
|                           | <b>mac</b>         | (Optional) Indicates that the MAC address of the MEP is specified.            |
|                           | <i>mac-address</i> | (Optional) MAC address in the format abcd.abcd.abcd.                          |

**Command Default** No remote MEPs are configured.

**Command Modes** Ethernet CFM configuration (config-ether-cfm)

|                        |                |                                                                 |
|------------------------|----------------|-----------------------------------------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                             |
|                        | 12.2(33)SRA    | This command was introduced.                                    |
|                        | 12.4(11)T      | This command was integrated into Cisco IOS Release 12.4(11)T.   |
|                        | 12.2(33)SXH    | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** Use the **mep crosscheck mpid vlan** command to statically configure remote MEPs that are part of a domain. These remote MEPs can be used in the cross-check operation. The cross-check operation only works when local MEPs are configured that correspond to the statically configured remote MEPs.

**Examples** The following example shows how to define a MEP within a maintenance domain with an ID of 20, in VLAN 5, and with MAC address a5a1.a5a1.a5a1:

```
Router(config-ether-cfm)# mep crosscheck mpid 20 vlan 5 mac a5a1.a5a1.a5a1
```



| Related Commands | Command                                                       | Description                                                                                                                       |
|------------------|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>ethernet cfm domain</b>                                    | Defines a CFM maintenance domain at a particular maintenance level.                                                               |
|                  | <b>ethernet cfm mep crosscheck</b>                            | Enables cross-checking between the list of configured remote MEPs of a domain and MEPs learned through CCMs.                      |
|                  | <b>ethernet cfm mep crosscheck start-delay</b>                | Configures the maximum amount of time that a device waits for remote MEPs to come up before the cross-check operation is started. |
|                  | <b>show ethernet cfm maintenance points remote crosscheck</b> | Displays information about remote maintenance points configured statically in a cross-check list.                                 |

## mode (ATM/T1/E1 controller)

To set the DSL controller into ATM mode and create an ATM interface or to set the T1 or E1 controller into T1 or E1 mode and create a logical T1/E1 controller, use the **mode** command in controller configuration mode. To disable the current mode and prepare to change modes, use the **no** form of this command.

**mode** {atm | cas}

**no mode** {atm | cas}

| Syntax Description | atm | <p>Sets the controller into ATM mode and creates an ATM interface (ATM 0). When ATM mode is enabled, no channel groups, DS0 groups, PRI groups, or time-division multiplexing (TDM) groups are allowed, because ATM occupies all the DS0s on the T1/E1 trunk.</p> <p>When you set the controller to ATM mode, the controller framing is automatically set to extended super frame (ESF) for T1 or cyclic redundancy check type 4 (CRC4) for E1. The line code is automatically set to binary 8-zero substitution (B8ZS) for T1 or high-density bipolar C (HDBC) for E1. When you remove ATM mode by entering the <b>no mode atm</b> command, ATM interface 0 is deleted.</p> <p><b>Note</b> The <b>mode atm</b> command without the <b>aim</b> keyword uses software to perform ATM segmentation and reassembly (SAR). This is supported on Cisco 2600 series WIC slots only; it is not supported on network module slots.</p> |
|--------------------|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | cas | <p>Sets the controller into Channel-associated signaling (CAS) mode. The T1 or E1 in this WIC slot is mapped to support T1 or E1 voice (that is, it is configured in a DS0 group or a PRI group).</p> <p>CAS mode is supported on both controller 0 and controller 1.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

**Command Default** The controller mode is disabled.

**Command Modes** Controller configuration

| Command History | Release     | Modification                                                                                                                                                                                                                          |
|-----------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 11.3 MA     | This command was introduced on the Cisco MC3810.                                                                                                                                                                                      |
|                 | 12.1(5)XM   | Support for this command was extended to the merged SGCP/MGCP software.                                                                                                                                                               |
|                 | 12.2(2)T    | This command was integrated into Cisco IOS Release 12.2(2)T.                                                                                                                                                                          |
|                 | 12.2(8)T    | This command was integrated into Cisco IOS Release 12.2(8)T for the Cisco IAD2420.                                                                                                                                                    |
|                 | 12.2(2)XB   | Support was extended to the Cisco 2600 series and Cisco 3660. The keyword <b>aim</b> and the argument <i>aim-slot</i> were added. The parenthetical modifier for the command was changed from “Voice over ATM” to “T1/E1 controller.” |
|                 | 12.2(15)T   | This command was implemented on the Cisco 2691 and the Cisco 3700 series.                                                                                                                                                             |
|                 | 12.3(4)XD   | This command was integrated into Cisco IOS Release 12.3(4)XD on Cisco 2600 series and Cisco 3700 series routers to configure DSL Frame mode and to add T1/E1 Framed support.                                                          |
|                 | 12.3(4)XG   | This command was integrated into Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers.                                                                                                                                        |
|                 | 12.3(7)T    | This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 2600 series and Cisco 3700 series routers.                                                                                                                       |
|                 | 12.3(11)T   | This command was implemented on Cisco 2800 and Cisco 3800 series routers.                                                                                                                                                             |
|                 | 12.3(14)T   | This command was implemented on Cisco 1800 series routers.                                                                                                                                                                            |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                                                                        |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not support DSL HWICs.                                                                                                                              |

### Usage Guidelines

When a DSL controller is configured in ATM mode, the mode must be configured identically on both the CO and CPE sides. Both sides must be set to ATM mode.



#### Note

If using the **no mode atm** command to leave ATM mode, the router must be rebooted immediately to clear the mode.

When configuring a DSL controller in T1 or E1 mode, the mode must be configured identically on the CPE and CO sides.

To disable ATM mode on the T1/E1 controller after configuring an ATM pseudowire, you must remove the **xconnect** statement from the ATM interface using the **no xconnect** command before issuing the **no mode atm** command on the controller.

### Examples

#### ATM Mode Example

The following example configures ATM mode on the DSL controller.

```
Router(config)# controller dsl 3/0
Router(config-controller)# mode atm
```

### CAS Mode Example

The following example configures T1 mode on the DSL controller.

```
Router(config)# controller t1 3/0  
Router(config-controller)# mode cas
```

#### Related Commands

| Command              | Description                                                                                             |
|----------------------|---------------------------------------------------------------------------------------------------------|
| <b>channel-group</b> | Configures a list of time slots for voice channels on controller T1 0 or E1 0.                          |
| <b>tdm-group</b>     | Configures a list of time slots for creating clear channel groups (pass-through) for TDM cross-connect. |

# mpls control-word

To enable the Multiprotocol Label Switching (MPLS) control word in an Any Transport over MPLS (AToM) static pseudowire connection, use the **mpls control-word** command in xconnect configuration mode. To disable the control word, use the **no** form of this command.

**mpls control-word**

**no mpls control-word**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The control word is included in connections.

**Command Modes** Xconnect configuration

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(33)SRB | This command was introduced.                                    |
|                 | 12.2(33)MRB | This command was integrated into Cisco IOS Release 12.2(33)MRB. |

**Usage Guidelines** This command is used when configuring AToM static pseudowires, and is mandatory when configuring Frame Relay data-link connection identifier (DLCI) and ATM adaptation layer 5 (AAL5) attachment circuits.

Because the control word is included by default, it may be necessary to explicitly disable this command in AToM static pseudowire configurations.

When the **mpls control-word** command is used in static pseudowire configurations, the command must be configured the same way on both ends of the connection to work correctly, or else the provider edge routers cannot exchange control messages to negotiate inclusion or exclusion of the control word.

**Examples** The following example shows the configuration for both sides of an AToM static pseudowire connection:

```
Router# configure terminal
Router(config)# interface Ethernet 1/0
Router(config-if)# xconnect 10.131.191.251 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 100 150
Router(config-if-xconn)# no mpls control-word
Router(config-if-xconn)# exit
Router(config-if)# exit
```

```
Router# configure terminal
Router(config)# interface Ethernet 1/0
Router(config-if)# xconnect 10.132.192.252 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 150 100
```

## mpls control-word

```
Router(config-if-xconn)# no mpls control-word
Router(config-if-xconn)# exit
Router(config-if)# exit
```

## Related Commands

| Command                         | Description                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>mpls label</b>               | Configures an AToM static pseudowire connection by defining local and remote pseudowire labels.                              |
| <b>mpls label range</b>         | Configures the range of local labels available for use on packet interfaces.                                                 |
| <b>show mpls l2transport vc</b> | Displays information about AToM VCs and AToM static pseudowires that have been enabled to route Layer 2 packets on a router. |
| <b>xconnect</b>                 | Binds an attachment circuit to a pseudowire, and configures an AToM static pseudowire.                                       |

# mpls ip (global configuration)

To enable Multiprotocol Label Switching (MPLS) forwarding of IPv4 packets along normally routed paths for the platform, use the **mpls ip** command in global configuration mode. To disable this feature, use the **no** form of this command.

**mpls ip**

**no mpls ip**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Label switching of IPv4 packets along normally routed paths is enabled for the platform.

**Command Modes** Global configuration

| Command History | Release     | Modification                                                                                                                                                                      |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.0(10)ST  | This command was introduced.                                                                                                                                                      |
|                 | 12.0(14)ST  | This command was integrated into Cisco IOS Release 12.0(14)ST.                                                                                                                    |
|                 | 12.1(2)T    | This command was integrated into Cisco IOS Release 12.1(2)T.                                                                                                                      |
|                 | 12.1(8a)E   | This command was integrated into Cisco IOS Release 12.1(8a)E.                                                                                                                     |
|                 | 12.2(2)T    | This command was integrated into Cisco IOS Release 12.2(2)T.                                                                                                                      |
|                 | 12.2(4)T    | This command was integrated into Cisco IOS Release 12.2(4)T.                                                                                                                      |
|                 | 12.2(8)T    | This command was integrated into Cisco IOS Release 12.2(8)T.                                                                                                                      |
|                 | 12.0(21)ST  | This command was integrated into Cisco IOS Release 12.0(21)ST.                                                                                                                    |
|                 | 12.0(22)S   | This command was integrated into Cisco IOS Release 12.0(22)S.                                                                                                                     |
|                 | 12.0(23)S   | This command was integrated into Cisco IOS Release 12.0(23)S.                                                                                                                     |
|                 | 12.2(14)S   | This command was integrated into Cisco IOS Release 12.2(14)S.                                                                                                                     |
|                 | 12.2(13)T   | This command was integrated into Cisco IOS Release 12.2(13)T.                                                                                                                     |
|                 | 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.                                                                     |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

**Usage Guidelines**

MPLS forwarding of IPv4 packets along normally routed paths (sometimes called dynamic label switching) is enabled by this command. For a given interface to perform dynamic label switching, this switching function must be enabled for the interface and for the platform.

The **no** form of this command stops dynamic label switching for all platform interfaces regardless of the interface configuration; it also stops distribution of labels for dynamic label switching. However, the **no** form of this command does not affect the sending of labeled packets through label switch path (LSP) tunnels.

For an LC-ATM interface, the **no** form of this command prevents the establishment of label virtual circuits (LVCs) originating at, terminating at, or passing through the platform.

**Examples**

The following example shows that dynamic label switching is disabled for the platform, and all label distribution is terminated for the platform:

```
Router(config)# no mpls ip
```

**Related Commands**

| Command                                  | Description                                                                                       |
|------------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>mpls ip (interface configuration)</b> | Enables MPLS forwarding of IPv4 packets along normally routed paths for the associated interface. |



# mpls ip (interface configuration)

To enable Multiprotocol Label Switching (MPLS) forwarding of IPv4 packets along normally routed paths for a particular interface, use the **mpls ip** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**mpls ip**

**no mpls ip**

**Syntax Description** This command has no arguments or keywords.

**Command Default** MPLS forwarding of IPv4 packets along normally routed paths for the interface is disabled.

**Command Modes** Interface configuration

| Command History | Release     | Modification                                                                                                                                                                      |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.0(10)ST  | This command was introduced.                                                                                                                                                      |
|                 | 12.0(14)ST  | This command was integrated into Cisco IOS Release 12.0(14)ST.                                                                                                                    |
|                 | 12.1(2)T    | This command was integrated into Cisco IOS Release 12.1(2)T.                                                                                                                      |
|                 | 12.1(8a)E   | This command was integrated into Cisco IOS Release 12.1(8a)E.                                                                                                                     |
|                 | 12.2(2)T    | This command was integrated into Cisco IOS Release 12.2(2)T.                                                                                                                      |
|                 | 12.2(4)T    | This command was integrated into Cisco IOS Release 12.2(4)T.                                                                                                                      |
|                 | 12.2(8)T    | This command was integrated into Cisco IOS Release 12.2(8)T.                                                                                                                      |
|                 | 12.0(21)ST  | This command was integrated into Cisco IOS Release 12.0(21)ST.                                                                                                                    |
|                 | 12.0(22)S   | This command was integrated into Cisco IOS Release 12.0(22)S.                                                                                                                     |
|                 | 12.0(23)S   | This command was integrated into Cisco IOS Release 12.0(23)S.                                                                                                                     |
|                 | 12.2(14)S   | This command was integrated into Cisco IOS Release 12.2(14)S.                                                                                                                     |
|                 | 12.2(13)T   | This command was integrated into Cisco IOS Release 12.2(13)T.                                                                                                                     |
|                 | 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.                                                                     |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

**Usage Guidelines**

MPLS forwarding of IPv4 packets along normally routed paths is sometimes called dynamic label switching. If dynamic label switching has been enabled for the platform when this command is issued on an interface, label distribution for the interface begins with the periodic transmission of neighbor discovery Hello messages on the interface. When the outgoing label for a destination routed through the interface is known, packets for the destination are labeled with that outgoing label and forwarded through the interface.

The **no** form of this command causes packets routed out through the interface to be sent unlabeled; this form of the command also terminates label distribution for the interface. However, the **no** form of the command does not affect the sending of labeled packets through any link-state packet (LSP) tunnels that might use the interface.

For an LC-ATM interface, the **no** form of this command prevents the establishment of label virtual circuits (LVCs) beginning at, terminating at, or passing through the interface.

**Examples**

The following example shows that label switching is enabled on the specified Ethernet interface:

```
Router(config)# configure terminal
Router(config-if)# interface e0/2
Router(config-if)# mpls ip
```

**Related Commands**

| Command                     | Description                                                                                                         |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>mpls ldp maxhops</b>     | Limits the number of hops permitted in an LSP established by the Downstream on Demand method of label distribution. |
| <b>show mpls interfaces</b> | Displays information about one or more interfaces that have been configured for label switching.                    |

# mpls label

To configure an Any Transport over MPLS (AToM) static pseudowire connection by defining local and remote circuit labels, use the **mpls label** command in xconnect configuration mode. To remove the local and remote pseudowire labels, use the **no** form of this command.

**mpls label** *local-pseudowire-label* *remote-pseudowire-label*

**no mpls label**

|                           |                                |                                                                                                 |
|---------------------------|--------------------------------|-------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>local-pseudowire-label</i>  | An unused static label that is within the range defined by the <b>mpls label range</b> command. |
|                           | <i>remote-pseudowire-label</i> | The value of the peer provider edge router's local pseudowire label.                            |

**Command Default** No default labels.

**Command Modes** Xconnect configuration

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                             |
|------------------------|----------------|-----------------------------------------------------------------|
|                        | 12.2(33)SRB    | This command was introduced.                                    |
|                        | 12.2(33)MRB    | This command was integrated into Cisco IOS Release 12.2(33)MRB. |

**Usage Guidelines** This command is mandatory when configuring AToM static pseudowires, and must be configured at both ends of the connection.

The **mpls label** command checks the validity of the local pseudowire label and generates an error message if the label is invalid.

**Examples** The following example shows configurations for both ends of an AToM static pseudowire connection:

```
Router# configure terminal
Router(config)# interface Ethernet 1/0
Router(config-if)# no ip address
Router(config-if)# xconnect 10.131.191.251 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 100 150
Router(config-if-xconn)# exit
Router(config-if)# exit

Router# configure terminal
Router(config)# interface Ethernet 1/0
Router(config-if)# no ip address
Router(config-if)# xconnect 10.132.192.252 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 150 100
Router(config-if-xconn)# exit
Router(config-if)# exit
```

| Related Commands | Command                         | Description                                                                                                                  |
|------------------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>mpls control-word</b>        | Enables sending the MPLS control word in an AToM static pseudowire connection.                                               |
|                  | <b>mpls label range</b>         | Configures the range of local labels available for use on packet interfaces.                                                 |
|                  | <b>show mpls l2transport vc</b> | Displays information about AToM VCs and AToM static pseudowires that have been enabled to route Layer 2 packets on a router. |
|                  | <b>xconnect</b>                 | Binds an attachment circuit to a pseudowire, and configures an AToM static pseudowire.                                       |

# mpls label range

To configure the range of local labels available for use with Multiprotocol Label Switching (MPLS) applications on packet interfaces, use the **mpls label range** command in global configuration mode. To revert to the platform defaults, use the **no** form of this command.

**mpls label range** *minimum-value maximum-value* [**static** *minimum-static-value maximum-static-value*]

**no mpls label range**

| Syntax Description          |  |                                                                                                                                                                                                                                              |
|-----------------------------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>minimum-value</i>        |  | The value of the smallest label allowed in the label space. The default is 16.                                                                                                                                                               |
| <i>maximum-value</i>        |  | The value of the largest label allowed in the label space. The default is platform-dependent.                                                                                                                                                |
| <b>static</b>               |  | (Optional) Reserves a block of local labels for static label assignments. If you omit the <b>static</b> keyword and the <i>minimum-static-value</i> and <i>maximum-static-value</i> arguments, no labels are reserved for static assignment. |
| <i>minimum-static-value</i> |  | (Optional) The minimum value for static label assignments. There is no default value.                                                                                                                                                        |
| <i>maximum-static-value</i> |  | (Optional) The maximum value for static label assignments. There is no default value.                                                                                                                                                        |

**Command Default** The platform's default values are used.

**Command Modes** Global configuration

| Command History | Release        | Modification                                                                                                                                                                                                                                    |
|-----------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 11.1CT         | This command was introduced.                                                                                                                                                                                                                    |
|                 | 12.1(3)T       | This command was modified to use the new MPLS Internet Engineering Task Force (IETF) terminology and command-line interface (CLI) syntax.                                                                                                       |
|                 | 12.0(23)S      | This command was integrated into Cisco IOS Release 12.0(23)S. The <b>static</b> keyword was added.                                                                                                                                              |
|                 | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                                                                                 |
|                 | 12.2(33)SXH    | This command was integrated into Cisco IOS Release 12.2(33)SXH.                                                                                                                                                                                 |
|                 | 12.4(16)       | The output was modified to display the upper and lower minimum static label values in the help lines instead of the default range.                                                                                                              |
|                 | 12.2(33)SB     | This command was integrated into Cisco IOS Release 12.2(33)SB.                                                                                                                                                                                  |
|                 | XE Release 2.2 | This command was integrated into Cisco IOS XE Release 2.2. The default values for the following arguments were modified: <i>maximum-value</i> , <i>minimum-static-value</i> , and <i>maximum-static-value</i> . The "Usage Guidelines" changed. |
|                 | 12.2(33)MRB    | This command was integrated into Cisco IOS Release 12.2(33)MRB.                                                                                                                                                                                 |

**Usage Guidelines**

The labels 0 through 15 are reserved by the IETF (see RFC 3032, MPLS Label Stack Encoding, for details) and cannot be included in the range specified in the **mpls label range** command. If you enter a 0 in the command, you get a message that indicates that the command is an unrecognized command.

The label range defined by the **mpls label range** command is used by all MPLS applications that allocate local labels (for dynamic label switching, MPLS traffic engineering, MPLS Virtual Private Networks (VPNs), and so on).

If you specify a new label range that does not overlap the range currently in use, the new range does not take effect until you reload the router or the router undergoes a Stateful Switchover (SSO) when you are using Cisco IOS Release 12.0S and older software. Later software with the new MPLS Forwarding Infrastructure (MFI), 12.2SR, 12.2SB, 12.2(33)XHI, 12.2(25)SE, and 12.5 allows immediate use of the new range. Existing label bindings, which may violate the newly-configured ranges, remain active until the binding is removed through other methods.

You can use label distribution protocols, such as Label Distribution Protocol (LDP) and Resource Reservation Protocol (RSVP), to reserve a generic range of labels from 16 through 1048575 for dynamic assignment.

You specify the optional keyword, **static**, to reserve labels for static assignment. The MPLS Static Labels feature requires that you configure a range of labels for static assignment. You can configure static bindings only from the current static range. If the static range is not configured or is exhausted, then you cannot configure static bindings.

The available range of label values is from 16 to 1048575. The maximum value defaults to 1048575, but might be limited to a lower value on certain platforms. Some platforms may support only 256,000 or 512,000 labels. Refer to your platform documentation for the default maximum label value.

If you configure the dynamic label space from 16 to 1048575, the static label space can be in a range that is outside the chosen dynamic label space. The upper and lower minimum static label values are displayed in the help line. For example, if you configure the dynamic label with a minimum value of 100 and a maximum value of 1000, the help lines display as follows:

```
Router(config)# mpls label range 100 1000 static ?

<1001-1048575>  Upper Minimum static label value
<16-99>         Lower Minimum static label value

Reserved Label Range --> 0      to 15
Available Label Range --> 16    to 1048575
Dynamic Label Range  --> 100    to 1000
Lower End Range      --> 16     to 99
Upper End Range      --> 1001   to 1048575
```

In this example, you can configure a static range from one of the following ranges: 16 to 99 or 1001 to 1048575.

If the lower minimum static label space is not available, the lower minimum is not displayed in the help line. For example:

```
Router(config)# mpls label range 16 400 static ?

<401-1048575>  Upper Minimum static label value
```

In this example, you can configure a static range with a minimum static value of 401 and a maximum static value of up to 1048575.

If an upper minimum static label space is not available, then the upper minimum is not displayed in the help line:

```
Router(config)# mpls label range 1000 1048575 static ?
```

<16-999> Lower Minimum static label value

In this example, the range available for static label assignment is from 16 to 999.

If you configure the dynamic label space with the default minimum (16) and maximum (1048575) values, no space remains for static label assignment, help lines are not displayed, and you cannot configure static label bindings. For example:

```
Router(config)# mpls label range 16 1048575 ?
<cr>
```

## Examples

The following example shows how to configure the size of the local label space. In this example, the minimum static value is set to 200, and the maximum static value is set to 120000.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# mpls label range 200 120000
Router(config)#
```

If you had specified a new range that overlaps the current range (for example, the new range of the minimum static value set to 16 and the maximum static value set to 120000), then the new range takes effect immediately.

The following example show how to configure a dynamic local label space with a minimum static value set to 1000 and the maximum static value set to 1048575 and a static label space with a minimum static value set to 16 and a maximum static value set to 999:

```
Router(config)# mpls label range 1000 1048575 static 16 999
Router(config)#
```

In the following output, the **show mpls label range** command, executed after a reload, shows that the configured range is now in effect:

```
Router# show mpls label range

Downstream label pool: Min/Max label: 1000/1048575
Range for static labels: Min/Max/Number: 16/999
```

The following example shows how to restore the label range to its default value:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# no mpls label range
Router(config)# end
```

## Related Commands

| Command                      | Description                                       |
|------------------------------|---------------------------------------------------|
| <b>show mpls label range</b> | Displays the range of the MPLS local label space. |

# mpls ldp router-id

To specify a preferred interface for the Label Distribution Protocol (LDP) router ID, use the **mpls ldp router-id** command in global configuration mode. To disable the interface from being used as the LDP router ID, use the **no** form of this command.

```

mpls ldp router-id [vrf vrf-name] interface [force]

no mpls ldp router-id [vrf vrf-name] [interface [force]]

```

## Syntax Description

|                            |                                                                                                                                                                                                     |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vrf</b> <i>vrf-name</i> | (Optional) Selects the interface as the LDP router ID for the named Virtual Private Network (VPN) routing and forwarding (VRF) table. The selected interface must be associated with the named VRF. |
| <i>interface</i>           | The specified interface to be used as the LDP router ID, provided that the interface is operational.                                                                                                |
| <b>force</b>               | (Optional) Alters the behavior of the <b>mpls ldp router-id</b> command, as described in theUsage Guidelines section.                                                                               |

## Command Default

- If the **mpls ldp router-id** command is not executed, the router determines the LDP router ID as follows:
1. The router examines the IP addresses of all operational interfaces.
  2. If these IP addresses include loopback interface addresses, the router selects the largest loopback address as the LDP router ID.
  3. Otherwise, the router selects the largest IP address pertaining to an operational interface as the LDP router ID.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.0(10)ST  | This command was introduced.                                    |
| 12.0(14)ST  | The <b>force</b> keyword was added.                             |
| 12.1(2)T    | This command was integrated into Cisco IOS Release 12.1(2)T.    |
| 12.1(8a)E   | This command was integrated into Cisco IOS Release 12.1(8a)E.   |
| 12.0(22)S   | This command was integrated into Cisco IOS Release 12.0(22)S.   |
| 12.4(5)     | The <b>vrf vrf-name</b> keyword and argument pair was added.    |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |



**Usage Guidelines**

The **mpls ldp router-id** command allows you to use the IP address of an interface as the LDP router ID. The following steps describe the normal process for determining the LDP router ID:

1. The router considers all the IP addresses of all operational interfaces.
2. If these addresses include loopback interface addresses, the router selects the largest loopback address. Configuring a loopback address helps ensure a stable LDP ID for the router, because the state of loopback addresses does not change. However, configuring a loopback interface and IP address on each router is not required.

The loopback IP address does not become the router ID of the local LDP ID under the following circumstances:

- If the loopback interface has been explicitly shut down.
- If the **mpls ldp router-id** command specifies that a different interface should be used as the LDP router ID.

If you use a loopback interface, make sure that the IP address for the loopback interface is configured with a /32 network mask. In addition, make sure that the routing protocol in use is configured to advertise the corresponding /32 network.

3. Otherwise, the router selects the largest interface address.

The router might select a router ID that is not usable in certain situations. For example, the router might select an IP address that the routing protocol cannot advertise to a neighboring router.

The router implements the router ID the next time it is necessary to select an LDP router ID. The effect of the command is delayed until the next time it is necessary to select an LDP router ID, which is typically the next time the interface is shut down or the address is deconfigured.

If you use the **force** keyword with the **mpls ldp router-id** command, the router ID takes effect more quickly. However, implementing the router ID depends on the current state of the specified interface:

- If the interface is up (operational) and its IP address is not currently the LDP router ID, the LDP router ID is forcibly changed to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.
- If the interface is down, the LDP router ID is forcibly changed to the IP address of the interface when the interface transitions to up. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.

The following behaviors apply to the default VRF as well as to VRFs that you explicitly configure with the **vrf vrf-name** keyword/argument pair:

- The interface you select as the router ID of the VRF must be associated with the VRF.
- If the interface is no longer associated with the VRF, the **mpls ldp router-id** command that uses the interface is removed.
- If the selected interface is deleted, the **mpls ldp router-id** command that uses the interface is removed.
- If you delete a VRF that you configured, the **mpls ldp router-id** command for the deleted VRF is removed. The default VRF cannot be deleted.

## Examples

The following example shows that the POS2/0/0 interface has been specified as the preferred interface for the LDP router ID. The IP address of that interface is used as the LDP router ID.

```
Router(config)# mpls ldp router-id pos2/0/0
```

The following example shows that the Ethernet 1/0 interface, which is associated with the VRF vpn-1, is the preferred interface. The IP address of the interface is used as the LDP router ID.

```
Router(config)# mpls ldp router-id vrf vpn-1 eth1/0
```

## Related Commands

| Command                        | Description                                       |
|--------------------------------|---------------------------------------------------|
| <b>show mpls ldp discovery</b> | Displays the status of the LDP discovery process. |

# neighbor (OSPF)

To configure Open Shortest Path First (OSPF) routers interconnecting to nonbroadcast networks, use the **neighbor** command in router address family topology or router configuration mode. To remove a configuration, use the **no** form of this command.

**neighbor** *ip-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter** **all**]

**no neighbor** *ip-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter** **all**]

| Syntax Description                  |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ip-address</i>                   | Interface IP address of the neighbor.                                                                                                                                                                                                                                                                                                                                                                                |
| <b>priority</b> <i>number</i>       | (Optional) Indicates the router priority value of the nonbroadcast neighbor associated with the IP address specified. The default is 0. This keyword does not apply to point-to-multipoint interfaces.                                                                                                                                                                                                               |
| <b>poll-interval</b> <i>seconds</i> | (Optional) Represents the poll interval time (in seconds). RFC 1247 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces. The range is from 0 to 4294967295 seconds.                                                                                                                             |
| <b>cost</b> <i>number</i>           | (Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured assumes the cost of the interface, based on the <b>ip ospf cost</b> command. For point-to-multipoint interfaces, the cost keyword and the <i>number</i> argument are the only options that are applicable. This keyword does not apply to nonbroadcast multiaccess (NBMA) networks. |
| <b>database-filter</b> <b>all</b>   | (Optional) Filters outgoing link-state advertisements (LSAs) to an OSPF neighbor.                                                                                                                                                                                                                                                                                                                                    |

**Command Default** This command is disabled by default. No configuration is specified.

**Command Modes** Router address family topology configuration (config-router-af-topology)  
Router configuration (config-router)

| Command History | Release     | Modification                                                                                                                                                                      |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 10.0        | This command was introduced.                                                                                                                                                      |
|                 | 11.3AA      | The <b>cost</b> keyword was added.                                                                                                                                                |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2(33)SRB | This command was made available in router address family topology configuration mode.                                                                                             |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

### Usage Guidelines

X.25 and Frame Relay provide an optional broadcast capability that can be configured in the map to allow OSPF to run as a broadcast network. At the OSPF level you can configure the router as a broadcast network. Refer to the **x25 map** and **frame-relay map** commands in the “X.25 Commands” and “Frame Relay Commands” chapters, respectively, in the *Cisco IOS Wide-Area Networking Command Reference* for more detail.

One neighbor entry must be included in the Cisco IOS software configuration for each known nonbroadcast network neighbor. The neighbor address must be on the primary address of the interface.

If a neighboring router has become inactive (hello packets have not been received for the Router Dead Interval period), it may still be necessary to send hello packets to the dead neighbor. These hello packets are sent at a reduced rate called *Poll Interval*.

When the router first starts up, it sends only hello packets to those routers with nonzero priority, that is, routers that are eligible to become designated routers (DRs) and backup designated routers (BDRs). After the DR and BDR are selected, DR and BDR starts sending hello packets to all neighbors in order to form adjacencies.



### Note

You cannot use the **neighbor (OSPF)** command to specify an Open Shortest Path First (OSPF) neighbor on non-broadcast networks within an OSPF Virtual Private Network (VPN) routing instance.

Prior to Cisco IOS Release 12.0, the **neighbor** command applied to NBMA networks only. With Release 12.0, the **neighbor** command applies to NBMA networks and point-to-multipoint networks. On NBMA networks, the **cost** keyword is not accepted.

### Release 12.2(33)SRB

If you plan to configure the Multi-Topology Routing (MTR) feature, you need to enter the **neighbor** command in router address family topology configuration mode in order for this OSPF router configuration command to become topology-aware.

### Examples

The following example declares a router at address 192.168.3.4 on a nonbroadcast network, with a priority of 1 and a poll interval of 180 seconds:

```
router ospf
 neighbor 192.168.3.4 priority 1 poll-interval 180
```

The following example illustrates a point-to-multipoint network with nonbroadcast:

```
interface Serial0
 ip address 10.0.1.1 255.255.255.0
 ip ospf network point-to-multipoint non-broadcast
 encapsulation frame-relay
 no keepalive
 frame-relay local-dlci 200
 frame-relay map ip 10.0.1.3 202
 frame-relay map ip 10.0.1.4 203
 frame-relay map ip 10.0.1.5 204
 no shut
!
```

```
router ospf 1
network 10.0.1.0 0.0.0.255 area 0
neighbor 10.0.1.3 cost 5
neighbor 10.0.1.4 cost 10
neighbor 10.0.1.5 cost 15
```

**Related Commands**

| Command                 | Description                                                                             |
|-------------------------|-----------------------------------------------------------------------------------------|
| <b>ip ospf priority</b> | Sets the router priority, which helps determine the designated router for this network. |

## neighbor remote-as (BGP)

To add an entry to the BGP or multiprotocol BGP neighbor table, use the **neighbor remote-as** command in router configuration mode. To remove an entry from the table, use the **no** form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number* ...]

**no neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number* ...]

|                           |                                 |                                                                                                              |
|---------------------------|---------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>ip-address</i>               | IP address of the neighbor.                                                                                  |
|                           | <i>peer-group-name</i>          | Name of a BGP peer group.                                                                                    |
|                           | <i>autonomous-system-number</i> | Number of an autonomous system to which the neighbor belongs in the range from 1 to 65535.                   |
|                           |                                 | For more details about autonomous system number formats, see the <b>router bgp</b> command.                  |
|                           |                                 | When used with the <b>alternate-as</b> keyword, up to five autonomous system numbers may be entered.         |
|                           | <b>alternate-as</b>             | (Optional) Specifies an alternate autonomous system in which a potential dynamic neighbor can be identified. |

**Command Default** There are no BGP or multiprotocol BGP neighbor peers.

**Command Modes** Router configuration (config-router)

| <b>Command History</b> | <b>Release</b>           | <b>Modification</b>                                                                                                                         |
|------------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
|                        |                          |                                                                                                                                             |
|                        | 10.0                     | This command was introduced.                                                                                                                |
|                        | 11.0                     | The <i>peer-group-name</i> argument was added.                                                                                              |
|                        | 11.1(20)CC               | The <b>nlri unicast</b> , <b>nlri multicast</b> , and <b>nlri unicast multicast</b> keywords were added.                                    |
|                        | 12.0(7)T                 | The <b>nlri unicast</b> , <b>nlri multicast</b> , and <b>nlri unicast multicast</b> keywords were removed.                                  |
|                        | 12.2(4)T                 | Support for the IPv6 address family was added.                                                                                              |
|                        | 12.2(25)SG               | This command was integrated into Cisco IOS Release 12.2(25)SG.                                                                              |
|                        | 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                             |
|                        | 12.2(33)SRB              | This command was modified. The <b>%</b> keyword was added.                                                                                  |
|                        | 12.2(33)SXH              | This command was integrated into Cisco IOS Release 12.2(33)SXH. The <b>alternate-as</b> keyword was added to support BGP dynamic neighbors. |
|                        | 12.2(33)SB               | This command was integrated into Cisco IOS Release 12.2(33)SB.                                                                              |
|                        | Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers.                                                                               |

| Release                  | Modification                                                                                                                                  |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(32)S12              | Support for 4-byte autonomous system numbers in asdot notation only was added.                                                                |
| 12.0(32)SY8              | This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.                              |
| 12.4(24)T                | This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.                                     |
| Cisco IOS XE Release 2.3 | This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.                                     |
| 12.2(33)SX11             | This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.                              |
| 12.0(33)S3               | This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain. |
| Cisco IOS XE Release 2.4 | This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain. |
| 12.4(20)MR               | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                |
| 12.2(33)MRA              | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                               |

### Usage Guidelines

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the **router bgp** global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group inherit the characteristic configured with this command.

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only unicast address prefixes. To exchange other address prefix types, such as multicast and Virtual Private Network (VPN) Version 4, neighbors must also be activated in the appropriate address family configuration mode.

To ensure a smooth transition, we recommend that all BGP speakers within an autonomous system that is identified using a 4-byte autonomous system number, be upgraded to support 4-byte autonomous system numbers.

### Examples

The following example specifies that a router at the address 10.108.1.2 is an internal BGP (iBGP) neighbor in autonomous system number 65200:

```
router bgp 65200
 network 10.108.0.0
 neighbor 10.108.1.2 remote-as 65200
```

The following example assigns a BGP router to autonomous system 65400, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured shares information about networks 10.108.0.0 and 192.168.7.0 with the neighbor routers. The first router is a remote router in a different autonomous system from the router on which this configuration is entered (an eBGP neighbor); the second **neighbor remote-as** command shows an internal BGP neighbor (with the same autonomous

■ **neighbor remote-as (BGP)**

system number) at address 10.108.234.2; and the last **neighbor remote-as** command specifies a neighbor on a different network from the router on which this configuration is entered (also an eBGP neighbor).

```
router bgp 65400
 network 10.108.0.0
 network 192.168.7.0
 neighbor 10.108.200.1 remote-as 65200
 neighbor 10.108.234.2 remote-as 65400
 neighbor 172.29.64.19 remote-as 65300
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only multicast routes:

```
router bgp 65001
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.31 1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
 address-family ipv4 multicast
  neighbor 10.108.1.1 activate
  neighbor 172.31 1.2 activate
  neighbor 172.16.2.2 activate
 exit-address-family
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only unicast routes:

```
router bgp 65001
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.31 1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
```

**Related Commands**

| Command           | Description                         |
|-------------------|-------------------------------------|
| <b>router bgp</b> | Configures the BGP routing process. |



# network-clock-select

The **network-clock-select** command names a source to provide timing for the network clock and to specify the selection priority for the clock source. To remove a network-clock-select configuration, use the **no** form of this command.

**network-clock-select** *priority* {*bits* | *sync* {*port*} | *packet\_timing*} {*E1* | *T1 slot/port*} {**10M** | **2.048M** | **1.544M**}

**no network-clock-select** *priority* {*bits* | *sync* {*port*} | *packet\_timing*} {*E1* | *T1 slot/port*}

## Syntax Description

|                      |                                                                             |
|----------------------|-----------------------------------------------------------------------------|
| <i>priority</i>      | Numeric value from 1 to 24 that specifies the priority of the clock source. |
| <b>bits</b>          | Specifies timing from a BITS port clock.                                    |
| <b>sync</b>          | Specifies timing using synchronous Ethernet.                                |
| <b>port</b>          | Specifies the port on which synchronous Ethernet is enabled.                |
| <b>packet_timing</b> | Enables packet timing using the RTM module.                                 |
| <b>E1</b>            | Specifies clocking using an E1 interface.                                   |
| <b>T1</b>            | Specifies clocking using a T1 interface.                                    |
| <i>slot/port</i>     | Specifies the slot and port of the interface used for timing.               |
| <b>10M</b>           | Specifies clocking at 10Mhz using the 10 Mhz timing port.                   |
| <b>2.048M</b>        | Specifies clocking at 2.048 Mhz using the 10 Mhz timing port.               |
| <b>1.544M</b>        | Specifies clocking at 1.544 Mhz using the 10 Mhz timing port.               |

## Command Default

There is no default setting.

## Command Modes

Global configuration

## Command History

| Release   | Modification                                                                                                                                  |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 11.3 MA   | This command was introduced on the Cisco MC3810.                                                                                              |
| 12.0(3)XG | The BVM as a possible network clock source was added.                                                                                         |
| 12.1(5)XM | This command was implemented on the Cisco 3660. The keywords t1 and e1 were introduced.                                                       |
| 12.2(4)T  | This command was integrated into Cisco IOS Release 12.2(4)T.                                                                                  |
| 12.2(2)XB | This command was implemented on the Cisco 2600 series and Cisco 3660 with AIMs installed.                                                     |
| 12.2(8)T  | This command was integrated into Cisco IOS Release 12.2(8)T.                                                                                  |
| 12.2(15)T | This command was implemented on the Cisco 2600XM, Cisco 2691, Cisco 3725, and Cisco 3745.                                                     |
| 12.3(8)T4 | This command was integrated into Cisco IOS Release 12.3(8)T4 and the bri keyword was added. Support was also added for the Cisco 2800 series. |

| Release     | Modification                                                                                                                                  |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 12.3(11)T   | This command was integrated into Cisco IOS Release 12.3(11)T and the atm keyword was added. Support was also added for the Cisco 3800 series. |
| 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2.                                                                               |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                               |

## Examples

The following example shows how to use the **network-clock-select** command:

```
Router# config t  
Router(config)# network-clock-select 1 packet_timing  
Router(config)# exit
```

## Related Commands

| Command                                  | Description                                       |
|------------------------------------------|---------------------------------------------------|
| <b>set network-clocks force-reselect</b> | Forces the router to re-select the network clock. |

# network-clock-select hold-timeout

The **network-clock-select hold-timeout** command specifies how long the router waits before reevaluating the network clock entry. To remove a **network-clock-select hold-timeout** configuration, use the **no** form of this command.

**network-clock-select hold-timeout** {*timeout* | **infinite**}

**no network-clock-select hold-timeout** {*timeout* | **infinite**}

## Syntax Description

|                 |                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>timeout</i>  | Value in seconds that specifies how long the router waits before reevaluating the network clock entry. Valid values are a number from 0 to 86400. |
| <b>infinite</b> | Specifies an infinite holdover.                                                                                                                   |

## Command Default

The default setting is **network-clock-select hold-timeout infinite**.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(19)MR2 | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Examples

The following example shows how to use the **network-clock-select** command:

```
Router# config t  
Router(config)# network-clock-select hold-timeout 2000  
Router(config)# exit
```

## Related Commands

| Command                                  | Description                                       |
|------------------------------------------|---------------------------------------------------|
| <b>set network-clocks force-reselect</b> | Forces the router to re-select the network clock. |

# network-clock-select hold-off-timeout

Determines that the time in milliseconds that the Cisco MWR 2941 waits when a synchronous Ethernet clock source fails before taking action. After the holdoff timer expires, the router announces the failure and takes one of the following actions depending on the clocking configuration:

- Considers other clock sources
- Switches to holdover mode—The router generates a timing signal based on the stored timing reference.

The **network-clock-select hold-timeout** command specifies how long the router waits before reevaluating the network clock entry. To remove a **network-clock-select hold-off-timeout** configuration, use the **no** form of this command.

**network-clock-select hold-timeout** *duration*

**no network-clock-select hold-timeout** *duration*

| <b>Syntax Description</b>                | <i>duration</i> Valid values are 0 or 50–10000                                                                                                                                                                      |         |              |                                          |                                                   |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|--------------|------------------------------------------|---------------------------------------------------|
| <b>Command Default</b>                   | The default setting is <b>network-clock-select hold-timeout infinite</b> .                                                                                                                                          |         |              |                                          |                                                   |
| <b>Command Modes</b>                     | Global configuration                                                                                                                                                                                                |         |              |                                          |                                                   |
| <b>Command History</b>                   | <table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>12.2(33)MRA</td><td>This command was introduced.</td></tr> </table>                                                                                | Release | Modification | 12.2(33)MRA                              | This command was introduced.                      |
| Release                                  | Modification                                                                                                                                                                                                        |         |              |                                          |                                                   |
| 12.2(33)MRA                              | This command was introduced.                                                                                                                                                                                        |         |              |                                          |                                                   |
| <b>Usage Guidelines</b>                  | The holdoff timer is a global timer value; it applies to both synchronous Ethernet clock sources when configured.                                                                                                   |         |              |                                          |                                                   |
| <b>Examples</b>                          | <p>The following example shows how to use the <b>network-clock-select</b> command:</p> <pre>Router# <b>config t</b> Router(config)# <b>network-clock-select hold-timeout 2000</b> Router(config)# <b>exit</b></pre> |         |              |                                          |                                                   |
| <b>Related Commands</b>                  | <table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td><b>set network-clocks force-reselect</b></td><td>Forces the router to re-select the network clock.</td></tr> </table>                               | Command | Description  | <b>set network-clocks force-reselect</b> | Forces the router to re-select the network clock. |
| Command                                  | Description                                                                                                                                                                                                         |         |              |                                          |                                                   |
| <b>set network-clocks force-reselect</b> | Forces the router to re-select the network clock.                                                                                                                                                                   |         |              |                                          |                                                   |

# network-clock-select input-stratum4

The **network-clock-select input-stratum4** command allows you to downgrade a clock source from Stratum 3 to Stratum 4. To configure a clock source as Stratum 3, use the **no** form of this command.

**network-clock-select input-stratum4**

**no network-clock-select input-stratum4**

## Command Default

The default setting is for onboard E1/T1 ports is Stratum 3; the default setting for E1/T1 HWIC ports is Stratum 4.



### Note

You cannot configure E1/T1 HWIC ports as Stratum 3.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(19)MR2 | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Examples

The following example shows how to use the **network-clock-select** command:

```
Router# config t  
Router(config)# network-clock-select input-stratum4  
Router(config)# exit
```

## Related Commands

| Command                                  | Description                                       |
|------------------------------------------|---------------------------------------------------|
| <b>set network-clocks force-reselect</b> | Forces the router to re-select the network clock. |

# network-clock-select mode

The **network-clock-select mode** command specifies the router switching mode. To remove a **network-clock-select mode** configuration, use the **no** form of this command.

**network-clock-select mode {revert | nonrevert}**

**no network-clock-select mode {revert | nonrevert}**

## Syntax Description

|                  |                                               |
|------------------|-----------------------------------------------|
| <b>nonrevert</b> | Sets the network clock to non-revertive mode. |
| <b>revert</b>    | Sets the network clock to revertive mode.     |

## Command Default

The default setting is **network-clock-select mode nonrevert**.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(19)MR2 | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Examples

The following example shows how to use the **network-clock-select** command:

```
Router# config t
Router(config)# network-clock-select mode revert
Router(config)# exit
```

## Related Commands

| Command                                  | Description                                       |
|------------------------------------------|---------------------------------------------------|
| <b>set network-clocks force-reselect</b> | Forces the router to re-select the network clock. |

# network-clock-select wait-to-restore-timeout

Specifies the amount of time in seconds that the Cisco MWR 2941 waits before considering a new clock source.

**network-clock-select wait-to-restore-timeout** *duration*

**no network-clock-select wait-to-restore-timeout** *duration*

|                           |                 |                                                                                                                                |
|---------------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>duration</i> | Specifies the timer value in seconds. Valid values are 0–720 (up to 12 minutes). The default value is 300 seconds (5 minutes). |
|---------------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------|

|                        |                                                                          |
|------------------------|--------------------------------------------------------------------------|
| <b>Command Default</b> | The default setting is <b>network-clock-select wait-to-restore 300</b> . |
|------------------------|--------------------------------------------------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

| <b>Command History</b> | Release     | Modification                                                    |
|------------------------|-------------|-----------------------------------------------------------------|
|                        | 12.2(33)MRA | This command was introduced.                                    |
|                        | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                                                                                                   |
|-------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | The restore timer is a global timer value; it applies to both synchronous Ethernet clock sources when configured. |
|-------------------------|-------------------------------------------------------------------------------------------------------------------|

|                 |                                                                                 |
|-----------------|---------------------------------------------------------------------------------|
| <b>Examples</b> | The following example shows how to use the <b>network-clock-select</b> command: |
|-----------------|---------------------------------------------------------------------------------|

```
Router# config t
Router(config)# network-clock-select wait-to-restore 360
Router(config)# exit
```

| <b>Related Commands</b> | Command                                  | Description                                       |
|-------------------------|------------------------------------------|---------------------------------------------------|
|                         | <b>set network-clocks force-reselect</b> | Forces the router to re-select the network clock. |

# payload-size

Specifies the size of the payload for packets on a structured CEM channel.

**payload-size** [*payload-size*]

## Syntax Description

*payload-size* Specifies the size of the payload for packets on a structured CEM channel. Valid values are 32 to 512. The default payload size for a T1 is 192 bytes; the default size for an E1 is 256 bytes.

**Note** The payload size must be a multiple of the number of timeslots for the CEM channel.

The default payload size is calculated as follows:

$8 \times \text{number of timeslots} \times 1 \text{ ms packetization delay}$

## Command Default

The default payload size for a structured CEM channel depends on the number of timeslots that constitute the channel. The default payload size for a T1 is 192 bytes; the default size for an E1 is 256 bytes.

## Command Modes

CEM circuit configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.3(7)T    | This command was introduced.                                    |
| 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Examples

The following example shows how to specify a sample rate:

```
Router# config t
Router(config)# interface cem 0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# payload-size 256
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```



| Related Commands | Command                | Description                                                                                                     |
|------------------|------------------------|-----------------------------------------------------------------------------------------------------------------|
|                  | <b>dejitter-buffer</b> | Configures the size of the dejitter buffer on a CEM channel.                                                    |
|                  | <b>idle-pattern</b>    | Specifies the data pattern transmitted on the T1/E1 line when missing packets are detected on the PWE3 circuit. |

# ping ethernet

To send Ethernet connectivity fault management (CFM) loopback messages to a destination maintenance endpoint (MEP), use the **ping ethernet** command in privileged EXEC mode.

**ping ethernet** {*mac-address* | **mpid** *mpid*} {**domain** *domain-name* [**vlan** *vlan-id*] [**source** *source-mpid*] [**level** *level-id*] [**vlan** *vlan-id*] }

## Syntax Description

|                    |                                                                         |
|--------------------|-------------------------------------------------------------------------|
| <i>mac-address</i> | MAC address of the destination MEP in the format abcd.abcd.abcd.        |
| <b>mpid</b>        | Specifies a maintenance point identifier.                               |
| <i>mpid</i>        | Integer from 1 to 8191 that identifies the MEP.                         |
| <b>domain</b>      | Specifies the domain where the destination MEP resides.                 |
| <i>domain-name</i> | String of a maximum of 154 characters that identifies the domain.       |
| <b>vlan</b>        | Specifies a VLAN.                                                       |
| <i>vlan-id</i>     | Integer from 1 to 4094 that identifies the VLAN.                        |
| <b>source</b>      | (Optional) Specifies a MEP's CoS that is sent in Ethernet CFM messages. |
| <i>source-mpid</i> | (Optional) Integer from 1 to 8191 that identifies the source MEP.       |
| <b>level</b>       | Indicates that a maintenance level is specified.                        |
| <i>level-id</i>    | Integer from 0 to 7 that identifies the maintenance level.              |

## Command Default

A CFM ping operation to the specified MEP is performed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release      | Modification                                                    |
|--------------|-----------------------------------------------------------------|
| 12.2(33)SX12 | This command was introduced.                                    |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

Use this command to test connectivity between MEPs.

If the continuity check database does not have entries for the specified MPID, an error message is displayed notifying you to use the **ping ethernet** *mac-address* command instead.

If a domain name has more than 43 characters, a warning message is displayed notifying you that the maintenance domain ID (MDID) are truncated to 43 characters in continuity check messages (CCMs) if "id <fmt> <MDID>" is not configured.

This command can be issued by specifying keywords and arguments as one command or as an "extended" command in which you specify options line by line.

## Examples

The following examples show how to send an Ethernet CFM loopback message to a destination MEP using the "extended ping" format:

Router# **ping**

```
Protocol [ip]: ethernet
Mac Address : aabb.cc03.bb99
Maintenance Domain : Domain_L5
VLAN [9]:
Source MPID [220]:
Repeat Count [5]:
Datagram Size [100]:
Timeout in seconds [5]:
Interval in seconds [0]:
Extended commands [n]:
Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages to aabb.cc03.bb99, timeout is 5 seconds:!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Router# **ping**

```
Protocol [ip]: ethernet
Multicast [n] : y
Maintenance Domain : Domain_L5
VLAN [9]:
Source MPID [220]:
Datagram Size [100]:
Timeout in seconds [5]:
Interval in seconds [0]:
Extended commands [n]:
Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages to 0180.c200.0035, timeout is 5 seconds:
Reply to Multicast request from aabb.cc03.bb99, 0 ms
```

Total Remote MEPs replied: 1

# ping ethernet vlan

To send Ethernet connectivity fault management (CFM) loopback messages to a maintenance endpoint (MEP) or maintenance intermediate point (MIP) destination, use the **ping ethernet vlan** command in privileged EXEC command mode.

**ping ethernet** {*mac-address* | *mpid*} {**domain** *domain-name* | **level** *level-id*} **vlan** *vlan-id* [**source** *mpid*]

|                           |                           |                                                                           |
|---------------------------|---------------------------|---------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>mac-address</i>        | MAC address of the remote maintenance point in the format abcd.abcd.abcd. |
|                           | <i>mpid</i>               | Integer from 0 to 8191 that identifies the MEP.                           |
|                           | <b>domain</b>             | Indicates a domain is specified.                                          |
|                           | <i>domain-name</i>        | String with a maximum of 154 characters that identifies the domain.       |
|                           | <b>level</b>              | Indicates that a maintenance level is specified.                          |
|                           | <i>level-id</i>           | Integer value of 0 to 7 that identifies the maintenance level.            |
|                           | <i>vlan-id</i>            | Integer value of 1 to 4094 that identifies the VLAN.                      |
|                           | <b>source</b> <i>mpid</i> | (Optional) Indicates a source maintenance point.                          |

**Command Default** A basic CFM ping operation to the specified MAC address (MEP or MIP) is performed.

**Command Modes** Privileged EXEC (#)

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                    |
|------------------------|----------------|--------------------------------------------------------------------------------------------------------|
|                        | 12.2(33)SRA    | This command was introduced.                                                                           |
|                        | 12.4(11)T      | The optional <b>source</b> keyword and <i>mpid</i> argument were added in Cisco IOS Release 12.4(11)T. |
|                        | 12.2(33)SXH    | This command was integrated into Cisco IOS Release 12.2(33)SXH.                                        |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                        |

**Usage Guidelines** A local MEP must be configured for the same level and VLAN before you can use this command.

The optional **source** keyword is available only when you enter a domain name. The **source** keyword is useful when there are multiple local MEPs in the same domain, level, and VLAN as the ping target. For outward facing MEPs, choosing the source MPID implicitly selects the interface from which the ping is sent.

**Examples**

The following example shows how to send an Ethernet CFM loopback message to MAC address 4123.pcef.9879 at maintenance level 3, VLAN ID 4325:

```
Router# ping ethernet 4123.pcef.9879 level 3 vlan 4325
```

**Related Commands**

| Command     | Description                                                                                                                         |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>ping</b> | Sends an echo request packet to an address, and then awaits a reply to determine whether a device can be reached or is functioning. |

## police (percent)

To configure traffic policing on the basis of a percentage of bandwidth available on an interface, use the **police** command in policy-map class configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

**police cir percent** *percentage* [*burst-in-msec*] [**bc** *conform-burst-in-msec ms*]  
 [**be** *peak-burst-in-msec ms*] [**pir percent** *percentage*] [**conform-action** *action* [**exceed-action**  
*action* [**violate-action** *action*]]]

**no police cir percent** *percentage* [*burst-in-msec*] [**bc** *conform-burst-in-msec ms*]  
 [**be** *peak-burst-in-msec ms*] [**pir percent** *percentage*] [**conform-action** *action* [**exceed-action**  
*action* [**violate-action** *action*]]]

### Syntax Description

|                              |                                                                                                                                                                                             |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>cir</b>                   | Indicates the committed information rate. Indicates that the CIR is used for policing traffic.                                                                                              |
| <b>percent</b>               | Specifies that a percentage of bandwidth is used for calculating the CIR.                                                                                                                   |
| <i>percentage</i>            | Specifies the bandwidth percentage. Valid range is a number from 1 to 100.                                                                                                                  |
| <i>burst-in-msec</i>         | (Optional) Burst in milliseconds. Valid range is a number from 1 to 2000.                                                                                                                   |
| <b>bc</b>                    | (Optional) The conform burst (bc) size used by the first token bucket for policing traffic.                                                                                                 |
| <i>conform-burst-in-msec</i> | (Optional) Specifies the bc value in milliseconds. Valid range is a number from 1 to 2000.                                                                                                  |
| <b>ms</b>                    | (Optional) Indicates that the burst value is specified in milliseconds.                                                                                                                     |
| <b>be</b>                    | (Optional) The Peak burst (be) size used by the second token bucket for policing traffic.                                                                                                   |
| <i>peak-burst-in-msec</i>    | (Optional) Specifies the be size in milliseconds. Valid range is a number from 1 to 2000.                                                                                                   |
| <b>pir</b>                   | (Optional) Peak information rate. Indicates that the PIR is used for policing traffic.                                                                                                      |
| <i>percent</i>               | (Optional) Specifies that a percentage of bandwidth is used for calculating the PIR.                                                                                                        |
| <b>conform-action</b>        | (Optional) Specifies the action taken on packets whose rate is less than the conform burst. You must specify a value for peak-burst-in-msec before you specify the <b>conform-action</b> .  |
| <b>exceed-action</b>         | (Optional) Specifies the action taken packets whose rate is within the conform and conform plus exceed burst.                                                                               |
| <b>violate-action</b>        | (Optional) Specifies the action taken on packets whose rate exceeds the conform plus exceed burst. You must specify the <b>exceed-action</b> before you specify the <b>violate-action</b> . |

*action* (Optional) Action to take on packets. Specify one of the following keywords:

#### All Supported Platforms

- **drop**—Drops the packet.
- **set-clp-transmit**—Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and sends the packet with the ATM CLP bit set to 1.
- **set-dscp-transmit** *new-dscp*—Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting.
- **set-frde-transmit**—Sets the Frame Relay discard eligible (DE) bit from 0 to 1 on the Frame Relay frame and sends the packet with the DE bit set to 1.
- **set-prec-transmit** *new-prec*—Sets the IP precedence and sends the packet with the new IP precedence value setting.
- **transmit**—Sends the packet with no alteration.

#### Supported Platforms Except the Cisco 10000 Series Router

- **policed-dscp-transmit**—(Exceed and violate action only). Changes the DSCP value per the policed DSCP map and sends the packet.
- **set-cos-inner-transmit** *value*—Sets the inner class of service field as a policing action for a bridged frame on the Enhanced FlexWAN module, and when using bridging features on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router.
- **set-cos-transmit** *value*—Sets the packet cost of service (CoS) value and sends the packet.
- **set-mpls-exposition-transmit**—Sets the Multiprotocol Label Switching (MPLS) experimental bits from 0 to 7 and sends the packet with the new MPLS experimental bit value setting.
- **set-mpls-topmost-transmit**—Sets the MPLS experimental bits on the topmost label and sends the packet.

#### Command Default

##### All Supported Platforms

The default bc and be values are 4 ms.

#### Command Modes

Policy-map class configuration (config-pmap-c)

#### Command History

| Release    | Modification                                                                        |
|------------|-------------------------------------------------------------------------------------|
| 12.0(5)XE  | This command was introduced.                                                        |
| 12.0(25)SX | The Percent-based Policing feature was introduced on the Cisco 10000 series router. |
| 12.1(1)E   | This command was integrated into Cisco IOS Release 12.2(1)E.                        |

| Release                  | Modification                                                                                                                                                                                                                                                                    |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.1(5)T                 | This command was integrated into Cisco IOS Release 12.1(5)T.                                                                                                                                                                                                                    |
| 12.2(13)T                | This command was modified for the Percentage-Based Policing and Shaping feature.                                                                                                                                                                                                |
| 12.0(28)S                | The command was integrated into Cisco IOS Release 12.0(28)S.                                                                                                                                                                                                                    |
| 12.2(18)SXE              | The command was integrated into Cisco IOS Release 12.2(18)SXE.                                                                                                                                                                                                                  |
| 12.2(28)SB               | The command was integrated into Cisco IOS Release 12.2(28)SB.                                                                                                                                                                                                                   |
| 12.2(33)SRA              | The <b>set-cos-inner-transmit</b> keyword for the <i>action</i> argument was added when using multipoint bridging (MPB) features on the Enhanced FlexWAN module, and when using MPB on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router. |
| 12.2(31)SB2              | Support was added on the PRE3 for the <b>set-frde-transmit</b> <i>action</i> argument for the Cisco 10000 series router.                                                                                                                                                        |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers.                                                                                                                                                                                                                  |
| 12.4(20)MR               | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                                                                                                                  |
| 12.2(33)MRA              | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                                                                                                                 |

## Usage Guidelines

This command calculates the cir and pir on the basis of a percentage of the maximum amount of bandwidth available on the interface. When a policy map is attached to the interface, the equivalent cir and pir values in bits per second (bps) are calculated on the basis of the interface bandwidth and the percent value entered with this command. The **show policy-map interface** command can then be used to verify the bps rate calculated.

The calculated cir and pir bps rates must be in the range of 8000 and 2000000000 bps. If the rates are outside this range, the associated policy map cannot be attached to the interface. If the interface bandwidth changes (for example, more is added), the bps values of the cir and the pir are recalculated on the basis of the revised amount of bandwidth. If the cir and pir percentages are changed after the policy map is attached to the interface, the bps values of the cir and pir are recalculated.

### Conform Burst and Peak Burst Sizes in Milliseconds

This command also allows you to specify the values for the conform burst size and the peak burst size in milliseconds. If you want bandwidth to be calculated as a percentage, the conform burst size and the peak burst size must be specified in milliseconds (ms).

### Hierarchical Policy Maps

Policy maps can be configured in two-level (nested) hierarchies; a top (or “parent”) level and a secondary (or “child”) level. The **police** (percent) command can be configured for use in either a parent or child policy map.

### Bandwidth and Hierarchical Policy Maps

The **police** (percent) command uses the maximum rate of bandwidth available as the reference point for calculating the bandwidth percentage. When the **police** (percent) command is configured in a child policy map, the **police** (percent) command uses the bandwidth amount specified in the next higher-level policy (in this case, the parent policy map). If the parent policy map does not specify the maximum bandwidth rate available, the **police** (percent) command uses the maximum bandwidth rate available on



the next higher level (in this case, the physical interface, the highest point in the hierarchy) as the reference point. The **police** (percent) command always looks to the next higher level for the bandwidth reference point. The following sample configuration illustrates this point:

```
Policymap parent_policy
  class parent
    shape average 512000
    service-policy child_policy

Policymap child_policy
  class normal_type
    police cir percent 30
```

In this sample configuration, there are two hierarchical policies: one called `parent_policy` and one called `child_policy`. In the policy map called `child_policy`, the `police` command has been configured in the class called `normal_type`. In this class, the percentage specified by for the **police** (percent) command is 30 percent. The command uses 512 kbps, the peak rate, as the bandwidth reference point for class `parent` in the `parent_policy`. The **police** (percent) command uses 512 kbps as the basis for calculating the cir rate (512 kbps \* 30 percent).

```
interface serial 4/0
  service-policy output parent_policy

Policymap parent_policy
  class parent
    bandwidth 512
    service-policy child_policy
```

In the above example, there is one policy map called `parent_policy`. In this policy map, a peak rate has not been specified. The **bandwidth** command has been used, but this command does not represent the maximum rate of bandwidth available. Therefore, the **police** (percent) command looks to the next higher level (in this case serial interface 4/0) to get the bandwidth reference point. Assuming the bandwidth of serial interface 4/0 is 1.5 Mbps, the **police** (percent) command uses 1.5 Mbps as the basis for calculating the cir rate (1500000 \* 30 percent).

### How Bandwidth Is Calculated

The **police** (percent) command is often used in conjunction with the **bandwidth** and **priority** commands. The **bandwidth** and **priority** commands can be used to calculate the total amount of bandwidth available on an entity (for example, a physical interface). When the **bandwidth** and **priority** commands calculate the total amount of bandwidth available on an entity, the following guidelines are invoked:

- If the entity is a physical interface, the total bandwidth is the bandwidth on the physical interface.
- If the entity is a shaped ATM permanent virtual circuit (PVC), the total bandwidth is calculated as follows:
  - For a variable bit rate (VBR) virtual circuit (VC), the sustained cell rate (SCR) is used in the calculation.
  - For an available bit rate (ABR) VC, the minimum cell rate (MCR) is used in the calculation.

For more information on bandwidth allocation, refer to the “Congestion Management Overview” chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

**Examples**

The following example shows how to configure traffic policing using a CIR and a PIR on the basis of a percentage of bandwidth. In this example, a CIR of 20 percent and a PIR of 40 percent have been specified. Additionally, an optional bc value and be value (300 ms and 400 ms, respectively) have been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40
Router(config-pmap-c-police)# exit
```

After the policy map and class maps are configured, the policy map is attached to an interface as shown in the following example:

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/0
Router(config-if)# service-policy input policy1
Router(config-if)# exit
```

**Related Commands**

| Command                             | Description                                                                                                                                                                         |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bandwidth (policy-map class)</b> | Specifies or modifies the bandwidth allocated for a class belonging to a policy map.                                                                                                |
| <b>bridge-domain</b>                | Enables RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged VLAN to an ATM PVC or Frame Relay DLCI.                                                             |
| <b>policy-map</b>                   | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                        |
| <b>priority</b>                     | Gives priority to a traffic class in a policy map.                                                                                                                                  |
| <b>service-policy</b>               | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.                                         |
| <b>shape (percent)</b>              | Specifies average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface.                                                                 |
| <b>show policy-map</b>              | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.                                                           |
| <b>show policy-map interface</b>    | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# police (policy map)

To create a per-interface policer and configure the policy-map class to use it, use the **police** command in policy-map class configuration mode. To delete the per-interface policer from the policy-map class, use the **no** form of this command.

## police

**police** *bps* [[**bc**] *normal-burst-bytes* [*maximum-burst-bytes* | [**be**] [*burst-bytes*]]] [**pir** *bps* [**be** *burst-bytes*]] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

**no police** *bps*

## police cir

**police cir** *bps* [[**bc**] *normal-burst-bytes* [*maximum-burst-bytes* | [**be**] [*burst-bytes*]]] [**pir** *bps* [**be** *burst-bytes*]] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

**no police cir** *bps*

## Syntax Description

|                                     |                                                                                                                                                                                                                                                |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>bps</i>                          | Target bit rate in bits per second (bps). The postfix values <b>k</b> , <b>m</b> , and <b>g</b> are allowed, as is a decimal point. Valid range is from 8000 (or 8k) to 64000000000 (or 64g).                                                  |
| <i>normal-burst-bytes</i>           | (Optional) CIR token-bucket size in bytes for handling a burst. Valid range is from 1000 to 512000000.                                                                                                                                         |
| <i>maximum-burst-bytes</i>          | (Optional) PIR token-bucket size in bytes for handling a burst. Valid range is from 1000 to 512000000.                                                                                                                                         |
| <i>burst-bytes</i>                  | (Optional) Token-bucket size in bytes for handling a burst. Valid range is from 1000 to 512000000.                                                                                                                                             |
| <b>bc</b>                           | (Optional) Specifies in bytes the allowed (conforming) burst size.                                                                                                                                                                             |
| <b>be</b>                           | (Optional) Specifies in bytes the allowed excess burst size.                                                                                                                                                                                   |
| <b>pir</b>                          | (Optional) Specifies the peak information rate (PIR).                                                                                                                                                                                          |
| <b>cir</b>                          | Specifies the committed information rate (CIR).                                                                                                                                                                                                |
| <b>conform-action</b> <i>action</i> | (Optional) Specifies the action to take on packets that conform to the rate limit. See the “Usage Guidelines” section for valid values for the <i>action</i> argument.                                                                         |
| <b>exceed-action</b> <i>action</i>  | (Optional) Specifies the action to be taken on packets when the packet rate is greater than the rate specified in the <i>maximum-burst-bytes</i> argument. See the “Usage Guidelines” section for valid values for the <i>action</i> argument. |
| <b>violate-action</b> <i>action</i> | (Optional) Specifies the action to be taken when the packet rate is greater than the rate specified in the <i>maximum-burst-bytes</i> argument. See the “Usage Guidelines” section for valid values for the <i>action</i> argument.            |
| <b>aggregate</b> <i>name</i>        | Specifies a previously defined aggregate policer name and configures the policy-map class to use the specified aggregate policer.                                                                                                              |
| <b>percent</b> <i>percent</i>       | Specifies the percentage of the interface bandwidth to be allowed. Valid range is from 1 to 100.                                                                                                                                               |

## police (policy map)

|                  |                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------|
| <i>burst</i>     | (Optional) Token-bucket size in milliseconds (ms) for handling a burst. Valid range is from 1 to 2000.         |
| <b>ms</b>        | Milliseconds. When bandwidth is specified as a percentage, this keyword must follow the <i>burst</i> argument. |
| <b>flow</b>      | Specifies a microflow policer that polices each flow.                                                          |
| <b>mask</b>      | Specifies the flow mask to be used for policing.                                                               |
| <b>dest-only</b> | Specifies the destination-only flow mask.                                                                      |
| <b>full-flow</b> | Specifies the full-flow mask.                                                                                  |
| <b>src-only</b>  | Specifies the source-only flow mask.                                                                           |

**Command Default** No policing is performed.

**Command Modes** Policy-map class configuration (config-pmap-c)

| Command History | Release       | Modification                                                                                                                                                                                                                                                                                                    |
|-----------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.2(14)SX    | This command was introduced on the Supervisor Engine 720.                                                                                                                                                                                                                                                       |
|                 | 12.2(17d)SXB  | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.                                                                                                                                                                                                     |
|                 | 12.2(17d)SXB3 | The <b>police bps</b> minimum rate was lowered from 32,000 to 8,000 on FlexWAN interfaces only.                                                                                                                                                                                                                 |
|                 | 12.2(18)SXD   | This command was changed as follows: <ul style="list-style-type: none"> <li>Added <b>set-mpls-exp-topmost-transmit</b> to the valid values for the <b>conform-action</b> keyword.</li> <li>Changed the <b>set-mpls-exp-transmit</b> keyword to <b>set-mpls-exp-imposition-transmit</b>.</li> </ul>              |
|                 | 12.2(18)SXE   | The <i>bps</i> maximum rate was increased from 4,000,000,000 to 10,000,000,000 bps to support 10-Gigabit Ethernet.                                                                                                                                                                                              |
|                 | 12.2(18)SXF   | The CIR maximum rate was increased to 10,000,000,000 bps.                                                                                                                                                                                                                                                       |
|                 | 12.2(33)SRA   | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                                                                                                                                                 |
|                 | 12.2(31)SB    | The command behavior was changed so that if you modify only the police rate parameters and not the police actions, the police actions default to the default actions: conform-action transmit, exceed-action drop, and violate-action drop. This was implemented on the Cisco 10000 series router for the PRE3. |
|                 | 12.2(33)SB    | The command behavior was changed so that if you modify only the police rate parameters and not the police actions, the police actions are preserved. This was implemented on the Cisco 10000 series router for the PRE3 and PRE4. For more information, see the Usage Guidelines section.                       |
|                 | 12.2(33)SXH2  | The CIR maximum rate was increased to 64,000,000,000 bps.                                                                                                                                                                                                                                                       |
|                 | 12.2(33)SXI   | The minimum CIR token bucket size was reduced to 1 byte.                                                                                                                                                                                                                                                        |
|                 | 12.4(20)MR    | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                                                                                                                                                  |
|                 | 12.2(33)MRA   | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                                                                                                                                                 |

## Usage Guidelines

In Cisco IOS Release 12.2(17d)SXB3, valid values for the *bps* argument for the FlexWAN interfaces only are from 8,000 to 4,000,000,000 bps.

Use the **mls qos aggregate-policer** *name* command to create a named aggregate policer.

You can create two types of aggregate policers: named and per-interface. Both types can be attached to more than one port as follows:

- You create named aggregate policers using the **mls qos aggregate-policer** command. If you attach a named aggregate policer to multiple ingress ports, it polices the matched traffic from all the ingress ports to which it is attached.
- You define per-interface aggregate policers in a policy-map class using the **police** command. If you attach a per-interface aggregate policer to multiple ingress ports, it polices the matched traffic on each ingress port separately.

Use the **no police aggregate** *name* command to clear the use of the named aggregate policer.

Enter the **police flow** command to define a microflow policer (you cannot apply microflow policing to ARP traffic).

Enter the **police** command to define per-interface (not named) aggregate policers.

If the traffic is both aggregate and microflow policed, the aggregate and the microflow policers must both be in the same policy-map class and each must use the same **conform-action** and **exceed-action** keywords.

## Values for the action Argument

The valid values for the *action* argument are as follows:

- **drop**—Drops packets that do not exceed the rate set for the *bps* argument.
- **set-clp-transmit**—Sets and sends the ATM cell loss priority (CLP).
- **set-cos-inner-transmit** {*new-cos*}—Marks the matched traffic with a new inner class of service (CoS) value of the *new-cos* argument. Valid values of the *new-cos* argument are from 0 to 7.
- **set-cos-transmit** {*new-cos*}—Marks the matched traffic with a new CoS value of the *new-cos* argument. Valid values of the *new-cos* argument are from 0 to 7.
- **set-cos-transmit**—Sets and sends the ATM cell loss priority (CLP).
- **set-dscp-transmit** {*dscp-bit-pattern* | *dscp-value* | **default** | **ef**}—Marks the matched traffic with a new DSCP value:
  - *dscp-bit-pattern*—Specifies a DSCP bit pattern. Valid values are listed in [Table 6](#).
  - *dscp-value*—Specifies a DSCP value. Valid values are from 0 to 63.
  - **default**—Matches packets with the default DSCP value (000000).
  - **ef**—Matches packets with the Expedited Forwarding (EF) per-hop behavior (PHB) DSCP value (101110).

**Table 6** Valid DSCP Bit Pattern Values

| Keyword     | Definition                                             |
|-------------|--------------------------------------------------------|
| <b>af11</b> | Matches packets with AF11 DSCP (001010).               |
| <b>af12</b> | Matches packets with AF12 DSCP (001100).               |
| <b>af13</b> | Matches packets with AF13 DSCP (001110).               |
| <b>af21</b> | Matches packets with AF21 DSCP (010010).               |
| <b>af22</b> | Matches packets with AF22 DSCP (010100).               |
| <b>af23</b> | Matches packets with AF23 DSCP (010110).               |
| <b>af31</b> | Matches packets with AF31 DSCP (011010).               |
| <b>af32</b> | Matches packets with AF32 DSCP (011100).               |
| <b>af33</b> | Matches packets with AF33 DSCP (011110).               |
| <b>af41</b> | Matches packets with AF41 DSCP (100010).               |
| <b>af42</b> | Matches packets with AF42 DSCP (100100).               |
| <b>af43</b> | Matches packets with AF43 DSCP (100110).               |
| <b>cs1</b>  | Matches packets with CS1 (precedence 1) DSCP (001000). |
| <b>cs2</b>  | Matches packets with CS2 (precedence 2) DSCP (010000). |
| <b>cs3</b>  | Matches packets with CS3 (precedence 3) DSCP (011000). |
| <b>cs4</b>  | Matches packets with CS4 (precedence 4) DSCP (100000). |
| <b>cs5</b>  | Matches packets with CS5 (precedence 5) DSCP (101000). |
| <b>cs6</b>  | Matches packets with CS6 (precedence 6) DSCP (110000). |
| <b>cs7</b>  | Matches packets with CS7 (precedence 7) DSCP (111000). |

- **set-frde-transmit**—Sets and sends the Frame Relay discard eligible (FR DE) bit. This is valid for the **exceed-action** *action* keyword and argument combination.
- **set-mpls-exp-imposition-transmit** *new-mpls-exp*—Rewrites the Multiprotocol Label Switching (MPLS) experimental (exp) bits on imposed label entries and transmits the bits. The *new-mpls-exp* argument specifies the value used to set the MPLS EXP bits that are defined by the policy map. Valid values for the *new-mpls-exp* argument are from 0 to 7.
- **set-mpls-exp-topmost-transmit**—Sets experimental bits on the topmost label and sends the packet.



**Note** The **set-mpls-exp-topmost-transmit** keyword is not supported in some releases of the Catalyst 6500 series switch or the Cisco 7600 series router.

- **set-prec-transmit** *new-precedence* [**exceed-action**]—Marks the matched traffic with a new IP-precedence value and transmits it. Valid values for the *new-precedence* argument are from 0 to 7. You can also follow this action with the **exceed-action** keyword.
- **set-qos-transmit**—Rewrites qos-group and sends the packet.
- **transmit**—Transmits the packets that do not exceed the rate set for the *bps* argument. The optional keyword and argument combination for the **transmit** keyword is **exceed-action** *action*.

If the following keywords are not specified, the default actions are as follows:

- **conform-action** is **transmit**.
- **exceed-action** is **drop**.
- **violate-action** is **drop**.

This example shows how to specify a previously defined aggregate-policer name and configure the policy-map class to use the specified aggregate policer:

```
Router(config-pmap-c)# police aggregate agg1
```

This example shows how to create a policy map named police-setting that uses the class map access-match, which is configured to trust received IP-precedence values and is configured with a maximum-capacity aggregate policer and a microflow policer:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 1000000000 200000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# police flow 10000000 10000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# exit
```

#### Related Commands

| Command                          | Description                                                                                                               |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>class-map</b>                 | Accesses QoS class-map configuration mode to configure QoS class maps.                                                    |
| <b>mls qos aggregate-policer</b> | Defines a named aggregate policer for use in policy maps.                                                                 |
| <b>police</b>                    | Configures traffic policing in QoS policy-map class configuration mode or QoS policy-map class police configuration mode. |
| <b>service-policy</b>            | Attaches a policy map to an interface.                                                                                    |
| <b>show class-map</b>            | Displays class-map information.                                                                                           |
| <b>show policy-map</b>           | Displays information about the policy map.                                                                                |
| <b>show policy-map interface</b> | Displays the statistics and the configurations of the input and output policies that are attached to an interface.        |

## police (two rates)

To configure traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR), use the **police** command in policy-map class configuration mode. To remove two-rate traffic policing from the configuration, use the **no** form of this command.

```
police cir cir [bc conform-burst] [pir pir] [be peak-burst] [conform-action action [exceed-action action [violate-action action]]]
```

```
no police cir
```

| Syntax Description    |  |                                                                                                                         |
|-----------------------|--|-------------------------------------------------------------------------------------------------------------------------|
| <b>cir</b>            |  | Committed information rate (CIR) at which the first token bucket is updated.                                            |
| <i>cir</i>            |  | CIR value in bits per second. The value is a number from 8000 to 200000000.                                             |
| <b>bc</b>             |  | (Optional) Conform burst (bc) size used by the first token bucket for policing.                                         |
| <i>conform-burst</i>  |  | (Optional) The bc value in bytes. The value is a number from 1000 to 51200000.                                          |
| <b>pir</b>            |  | (Optional) Peak information rate (PIR) at which the second token bucket is updated.                                     |
| <i>pir</i>            |  | (Optional) Specifies the PIR value in bits per second. The value is a number from 8000 to 200000000.                    |
| <b>be</b>             |  | (Optional) Peak burst (be) size used by the second token bucket for policing.                                           |
| <i>peak-burst</i>     |  | (Optional) Specifies the peak burst (be) size in bytes. The size varies according to the interface and platform in use. |
| <b>conform-action</b> |  | (Optional) Action to take on packets that conform to the CIR and PIR.                                                   |
| <b>exceed-action</b>  |  | (Optional) Action to take on packets that conform to the PIR but not the CIR.                                           |



|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>violate-action</b> | (Optional) Action to take on packets exceed the PIR.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <i>action</i>         | (Optional) Action to take on packets. Specify one of the following keywords: <ul style="list-style-type: none"> <li>• <b>drop</b>—Drops the packet.</li> <li>• <b>set-clp-transmit</b>—Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and sends the packet with the ATM CLP bit set to 1.</li> <li>• <b>set-cos-inner-transmit</b> <i>value</i>—Sets the inner class of service field as a policing action for a bridged frame on the Enhanced FlexWAN module, and when using bridging features on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router.</li> <li>• <b>set-dscp-transmit</b> <i>new-dscp</i>—Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting.</li> <li>• <b>set-dscp-tunnel-transmit</b> <i>value</i>—Sets the DSCP value (0 to 63) in the tunnel header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) or Generic Routing Encapsulation (GRE) tunneled packet for tunnel marking and transmits the packet with the new value.</li> <li>• <b>set-frde-transmit</b>—Sets the Frame Relay discard eligible (DE) bit from 0 to 1 on the Frame Relay frame and sends the packet with the DE bit set to 1.</li> <li>• <b>set-mpls-exp-transmit</b>—Sets the Multiprotocol Label Switching (MPLS) experimental bits from 0 to 7 and sends the packet with the new MPLS experimental bit value setting.</li> <li>• <b>set-prec-transmit</b> <i>new-prec</i>—Sets the IP precedence and sends the packet with the new IP precedence value setting.</li> <li>• <b>set-prec-tunnel-transmit</b> <i>value</i>—Sets the precedence value (0 to 7) in the tunnel header of an L2TPv3 or GRE tunneled packet for tunnel marking and transmits the packet with the new value.</li> <li>• <b>set-qos-transmit</b> <i>new-qos</i>—Sets the quality of service (QoS) group value and sends the packet with the new QoS group value setting.</li> <li>• <b>transmit</b>—Sends the packet with no alteration.</li> </ul> |

|                        |                                               |
|------------------------|-----------------------------------------------|
| <b>Command Default</b> | Traffic policing using two rates is disabled. |
|------------------------|-----------------------------------------------|

|                      |                                                |
|----------------------|------------------------------------------------|
| <b>Command Modes</b> | Policy-map class configuration (config-pmap-c) |
|----------------------|------------------------------------------------|

|                        |                |                                                                                                           |
|------------------------|----------------|-----------------------------------------------------------------------------------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                       |
|                        | 12.0(5)XE      | This command was introduced.                                                                              |
|                        | 12.1(1)E       | This command was integrated into Cisco IOS Release 12.1(1)E.                                              |
|                        | 12.1(5)T       | This command was integrated into Cisco IOS Release 12.1(5)T. The <b>violate-action</b> keyword was added. |

| Release     | Modification                                                                                                                                                                                                                                                                                        |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(2)T    | The following keywords for the <i>action</i> argument were added: <ul style="list-style-type: none"> <li>• <b>set-clp-transmit</b></li> <li>• <b>set-frde-transmit</b></li> <li>• <b>set-mpls-exp-transmit</b></li> </ul>                                                                           |
| 12.2(4)T    | This command expanded for the Two-Rate Policing feature. The <b>cir</b> and <b>pir</b> keywords were added to accommodate two-rate traffic policing.                                                                                                                                                |
| 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB, and the <b>set-dscp-tunnel-transmit</b> and <b>set-prec-tunnel-transmit</b> keywords for the <i>action</i> argument were added. These keywords are intended for marking Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunneled packets. |
| 12.2(33)SRA | The <b>set-cos-inner-transmit</b> keyword for the <i>action</i> argument was added when using multipoint bridging (MPB) features on the Enhanced FlexWAN module, and when using MPB on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router.                     |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.                                                                                                                   |
| 12.2(33)SRC | This command was modified to support the Cisco 7600 series router equipped with a Cisco Multilayer Switch Feature Card 3 (MSFC3).                                                                                                                                                                   |
| 12.4(15)T2  | This command was modified to include support for marking Generic Routing Encapsulation (GRE) tunneled packets. <p><b>Note</b> For this release, marking GRE-tunneled packets is supported only on platforms equipped with a Cisco MGX Route Processor Module (RPM-XF).</p>                          |
| 12.2(33)SB  | This command was modified to include support for marking GRE-tunneled packets, and support for the Cisco 7300 series router was added.                                                                                                                                                              |
| 12.4(20)T   | Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).                                                                                                                                                          |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                                                                                                                                      |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                                                                                                                                     |

## Usage Guidelines

### Configuring Priority with an Explicit Policing Rate

When you configure a priority class with an explicit policing rate, traffic is limited to the policer rate regardless of congestion conditions. In other words, even if bandwidth is available, the priority traffic cannot exceed the rate specified with the explicit policer.

### Token Buckets

Two-rate traffic policing uses two token buckets—Tc and Tp—for policing traffic at two independent rates. Note the following points about the two token buckets:

- The Tc token bucket is updated at the CIR value each time a packet arrives at the two-rate policer. The Tc token bucket can contain up to the conform burst (Bc) value.
- The Tp token bucket is updated at the PIR value each time a packet arrives at the two-rate policer. The Tp token bucket can contain up to the peak burst (Be) value.

### Updating Token Buckets

The following scenario illustrates how the token buckets are updated:

A packet of B bytes arrives at time t. The last packet arrived at time t1. The CIR and the PIR token buckets at time t are represented by Tc(t) and Tp(t), respectively. Using these values and in this scenario, the token buckets are updated as follows:

$$Tc(t) = \min(CIR * (t-t1) + Tc(t1), Bc)$$

$$Tp(t) = \min(PIR * (t-t1) + Tp(t1), Be)$$

### Marking Traffic

The two-rate policer marks packets as either conforming, exceeding, or violating a specified rate. The following points (using a packet of B bytes) illustrate how a packet is marked:

- If  $B > Tp(t)$ , the packet is marked as violating the specified rate.
- If  $B > Tc(t)$ , the packet is marked as exceeding the specified rate, and the  $Tp(t)$  token bucket is updated as  $Tp(t) = Tp(t) - B$ .

Otherwise, the packet is marked as conforming to the specified rate, and both token buckets— $Tc(t)$  and  $Tp(t)$ —are updated as follows:

$$Tp(t) = Tp(t) - B$$

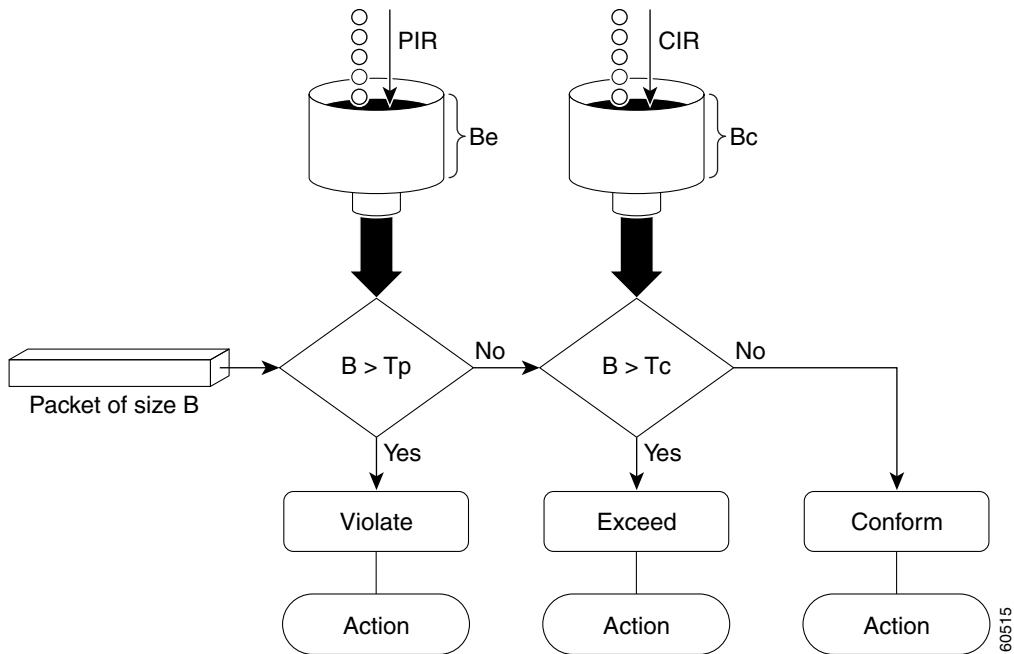
$$Tc(t) = Tc(t) - B$$

For example, if the CIR is 100 kbps, the PIR is 200 kbps, and a data stream with a rate of 250 kbps arrives at the two-rate policer, the packet would be marked as follows:

- 100 kbps would be marked as conforming to the rate.
- 100 kbps would be marked as exceeding the rate.
- 50 kbps would be marked as violating the rate.

### Marking Packets and Assigning Actions Flowchart

The flowchart in [Figure 1](#) illustrates how the two-rate policer marks packets and assigns a corresponding action (that is, violate, exceed, or conform) to the packet.

**Figure 1** *Marking Packets and Assigning Actions with the Two-Rate Policer*

## Examples

### Setting Priority with an Explicit Policing Rate

In the following example, priority traffic is limited to a committed rate of 1000 kbps regardless of congestion conditions in the network:

```

Router(config)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# police cir 1000000 conform-action transmit exceed-action drop

```

### Two-Rate Policing

In the following example, two-rate traffic policing is configured on a class to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps:

```

Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial0/1
Router(config-if)# service-policy output policy1
Router(config-if)# end
Router# show policy-map policy1

Policy Map policy1
Class police
  police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop

```

Traffic marked as conforming to the average committed rate (500 kbps) is sent as is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, is marked with IP Precedence 2 and then sent. All traffic marked as exceeding 1 Mbps is dropped. The burst parameters are set to 10000 bytes.

In the following example, 1.25 Mbps of traffic is sent (“offered”) to a policer class:

```
Router# show policy-map interface serial3/0
```

```
Serial3/0
```

```
Service-policy output: policy1
```

```
Class-map: police (match all)
```

```
148803 packets, 36605538 bytes
```

```
30 second offered rate 1249000 bps, drop rate 249000 bps
```

```
Match: access-group 101
```

```
police:
```

```
cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
```

```
conformed 59538 packets, 14646348 bytes; action: transmit
```

```
exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
```

```
violated 29731 packets, 7313826 bytes; action: drop
```

```
conformed 499000 bps, exceed 500000 bps violate 249000 bps
```

```
Class-map: class-default (match-any)
```

```
19 packets, 1990 bytes
```

```
30 seconds offered rate 0 bps, drop rate 0 bps
```

```
Match: any
```

The two-rate policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming to the rate are sent as is, and packets marked as exceeding the rate are marked with IP Precedence 2 and then sent. Packets marked as violating the rate are dropped.

## Related Commands

| Command                          | Description                                                                                                                                                                         |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>police</b>                    | Configures traffic policing.                                                                                                                                                        |
| <b>policy-map</b>                | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                        |
| <b>service-policy</b>            | Attaches a policy map to an input interface or an output interface to be used as the service policy for that interface.                                                             |
| <b>show policy-map</b>           | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.                                                           |
| <b>show policy-map interface</b> | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

## police rate (control-plane)

To configure traffic policing for traffic that is destined for the control plane, use the **police rate** command in QoS policy-map class configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

**police rate** *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**]  
 [**peak-burst** *peak-burst-in-packets* **packets**] [**conform-action** *action*]

**no police rate** *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**]  
 [**peak-burst** *peak-burst-in-packets* **packets**] [**conform-action** *action*]

### Syntax for Percent

**police rate percent** *percentage* [**burst** *ms ms*] [**peak-rate percent** *percentage*] [**peak-burst** *ms ms*]

**no police rate percent** *percentage* [**burst** *ms ms*] [**peak-rate percent** *percentage*] [**peak-burst** *ms ms*]

### Syntax Description

|                                                               |                                                                                                                                                                                                             |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>units</b>                                                  | Specifies the police rate. If the police rate is specified in pps, the valid range of values is 1 to 2000000 pps. If the police rate is specified in bps, the valid range of values is 8000 to 20000000000. |
| <b>pps</b>                                                    | Specifies that packets per seconds (pps) is used to determine the rate at which traffic is policed.                                                                                                         |
| <b>burst</b> <i>burst-in-packets</i> <b>packets</b>           | (Optional) Specifies the burst rate, in packets, used for policing traffic. Valid range of values is 1 to 512000.                                                                                           |
| <b>peak-rate</b> <i>peak-rate-in-pps</i> <b>pps</b>           | (Optional) Specifies the peak information rate (PIR) used for policing traffic and calculating the PIR. Valid range of values is 1 to 512000.                                                               |
| <b>peak-burst</b> <i>peak-burst-in-packets</i> <b>packets</b> | (Optional) Specifies the peak burst value, in packets, used for policing traffic. Valid range of values is 1 to 512000.                                                                                     |
| <b>bps</b>                                                    | (Optional) Specifies that bits per second (bps) is used to determine the rate at which traffic is policed.                                                                                                  |
| <b>burst</b> <i>burst-in-bytes</i> <b>bytes</b>               | (Optional) Specifies the burst rate, in bytes, used for policing traffic. Valid range is from 1000 to 512000000.                                                                                            |
| <b>peak-rate</b> <i>peak-rate-in-bps</i> <b>bps</b>           | (Optional) Specifies the peak burst value, in bytes, for the peak rate. Valid range is from 1000 to 512000000.                                                                                              |
| <b>peak-burst</b> <i>peak-burst-in-bytes</i> <b>bytes</b>     | (Optional) Specifies the peak burst value, in bytes, used for policing traffic. Valid range is from 1000 to 512000000.                                                                                      |
| <b>percent</b>                                                | A percentage of interface bandwidth used to determine the rate at which traffic is policed.                                                                                                                 |
| <i>percentage</i>                                             | Specifies the bandwidth percentage. Valid range is from 1 to 100.                                                                                                                                           |
| <b>burst</b> <i>ms ms</i>                                     | (Optional) Specifies the burst rate, in milliseconds, used for policing traffic. Valid range is from 1 to 2000.                                                                                             |
| <b>peak-rate percent</b> <i>percentage</i>                    | (Optional) Specifies a percentage of interface bandwidth used to determine the PIR. Valid range is from 1 to 100.                                                                                           |
| <b>peak-burst</b> <i>ms ms</i>                                | (Optional) Specifies the peak burst rate, in milliseconds, used for policing traffic. Valid range is from 1 to 2000.                                                                                        |

|                                     |                                                                                                                                                                        |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>conform-action</b> <i>action</i> | (Optional) Specifies the action to take on packets that conform to the police rate limit. See the “Usage Guidelines” section for the actions you can specify.          |
| <b>exceed-action</b> <i>action</i>  | (Optional) Specifies the action to take on packets that exceed the rate limit. See the “Usage Guidelines” section for the actions you can specify.                     |
| <b>violate-action</b> <i>action</i> | (Optional) Specifies the action to take on packets that continuously exceed the police rate limit. See the “Usage Guidelines” section for the actions you can specify. |

**Command Default** Disabled

**Command Modes** QoS policy-map class configuration

| Command History | Release      | Modification                                                                                                     |
|-----------------|--------------|------------------------------------------------------------------------------------------------------------------|
|                 | 12.3(7)T     | This command was introduced.                                                                                     |
|                 | 12.2(18)SXD1 | Support for this command was introduced on the Supervisor Engine 720.                                            |
|                 | 12.2(25)S    | This command was integrated into Cisco IOS Release 12.2(25)S.                                                    |
|                 | 12.2(33)SRA  | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                  |
|                 | 12.2(31)SB2  | This command was integrated into Cisco IOS Release 12.2(31)SB2 and implemented on the Cisco 10000 series router. |
|                 | 12.3(7)T     | This command was introduced.                                                                                     |
|                 | 12.4(20)MR   | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                   |
|                 | 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                  |

**Usage Guidelines** Use the **police rate** command to limit traffic that is destined for the control plane on the basis of packets per second (pps), bytes per seconds (bps), or a percentage of interface bandwidth.

If the **police rate** command is issued, but the a rate is not specified, traffic that is destined for the control plane is policed on the basis of bps.

[Table 7](#) lists the actions you can specify for the *action* argument.

**Table 7** *action* Argument Values

| Action                                         | Description                                                                                                                             |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>drop</b>                                    | Drops the packet. This is the default action for traffic that exceeds or violates the committed police rate.                            |
| <b>set-clp-transmit</b> <i>value</i>           | Sets the ATM Cell Loss Priority (CLP) bit on the ATM cell. Valid values are 0 or 1.                                                     |
| <b>set-discard-class-transmit</b> <i>value</i> | Sets the discard class attribute of a packet and transmits the packet with the new discard class setting. Valid values are from 0 to 7. |

**Table 7** *action Argument Values (continued)*

| Action                                               | Description                                                                                                                                                                                        |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>set-dscp-transmit</b> <i>value</i>                | Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value setting. Valid values are from 0 to 63.                                            |
| <b>set-dscp-tunnel-transmit</b> <i>value</i>         | Rewrites the tunnel packet DSCP and transmits the packet with the new tunnel DSCP value. Valid values are from 0 to 63.                                                                            |
| <b>set-frde-transmit</b> <i>value</i>                | Sets the Frame Relay Discard Eligibility (DE) bit from 0 to 1 on the Frame Relay frame and transmits the packet with the DE bit set to 1.                                                          |
| <b>set-mpls-exp-imposition-transmit</b> <i>value</i> | Sets the Multiprotocol Label Switching (MPLS) experimental (EXP) bits in the imposed label headers and transmits the packet with the new MPLS EXP bit value setting. Valid values are from 0 to 7. |
| <b>set-mpls-exp-transmit</b> <i>value</i>            | Sets the MPLS EXP field value in the MPLS label header at the input interface, output interface, or both. Valid values are from 0 to 7.                                                            |
| <b>set-prec-transmit</b> <i>value</i>                | Sets the IP precedence and transmits the packet with the new IP precedence value. Valid values are from 0 to 7.                                                                                    |
| <b>set-prec-tunnel-transmit</b> <i>value</i>         | Sets the tunnel packet IP precedence and transmits the packet with the new IP precedence value. Valid values are from 0 to 7.                                                                      |
| <b>set-qos-transmit</b> <i>value</i>                 | Sets the QoS group and transmits the packet with the new QoS group value. Valid values are from 0 to 63.                                                                                           |
| <b>transmit</b>                                      | Transmits the packet. The packet is not altered.                                                                                                                                                   |

**Examples**

The following example shows how to configure the action to take on packets that conform to the police rate limit:

```
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
Router(config)# access-list 140 permit tcp any any eq telnet
Router(config)# class-map match-any pps-1
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map copp-pps
Router(config-pmap)# class pps-1
Router(config-pmap)# police rate 10000 pps burst 100 packets peak-rate 10100 pps
peak-burst 150 packets conform-action transmit
Router(config-cmap)# exit
Router(config)# control-plane
Router(config-cp)# service-policy input copp-pps
Router(config-cp)# exit
```

**Related Commands**



| Command                | Description                                                                                                               |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>policy-map</b>      | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.              |
| <b>show policy-map</b> | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |

# policy-map

To enter policy-map configuration mode and create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map** command in global configuration mode. To delete a policy map, use the **no** form of this command.

**policy-map** [**type** { **control** | **service** }] *policy-map-name*

**no policy-map** [**type** { **control** | **traffic** }] *policy-map-name*

## Syntax Description

|                        |                                                                                  |
|------------------------|----------------------------------------------------------------------------------|
| <b>type</b>            | Specifies the policy-map type.                                                   |
| <b>control</b>         | (Optional) Creates a control policy map.                                         |
| <b>service</b>         | (Optional) Creates a service policy map.                                         |
| <i>policy-map-name</i> | Name of the policy map. The name can be a maximum of 40 alphanumeric characters. |

## Command Default

The policy map is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release     | Modification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(5)T    | This command was introduced.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 12.4(4)T    | The <b>type access-control</b> keywords were added to support flexible packet matching. The <b>type port-filter</b> and <b>type queue-threshold</b> keywords were added to support control-plane protection.                                                                                                                                                                                                                                                                                                                                                |
| 12.4(6)T    | The <b>type logging</b> keywords were added to support control-plane packet logging.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 12.2(31)SB  | The <b>type control</b> and <b>type service</b> keywords were added to support the Cisco 10000 series router.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 12.2(18)ZY  | The following modifications were made to the <b>policy-map</b> command: <ul style="list-style-type: none"> <li>The <b>type access-control</b> keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series switch that is equipped with the Supervisor 32/programmable intelligent services accelerator (PISA) engine.</li> <li>The command was modified to enhance Network-Based Application Recognition (NBAR) functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/PISA engine.</li> </ul> |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.                                                                                                                                                                                                                                                                                                                                                                           |
| 12.2(33)SRC | Support for this command was implemented on Cisco 7600 series routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Release                  | Modification                                                                                                                                         |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers.                                                                                       |
| 12.4(20)MR               | This command was integrated into Cisco IOS Release 12.4(20)MR. This release only supports the <b>type control</b> and <b>type service</b> keywords.  |
| 12.2(33)MRA              | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release only supports the <b>type control</b> and <b>type service</b> keywords. |

### Usage Guidelines

Use the **policy-map** command to specify the name of the policy map to be created, added to, or modified before you configure policies for classes whose match criteria are defined in a class map. The **policy-map** command enters policy-map configuration mode, in which you can configure or modify the class policies for a policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. Use the **class-map** and **match** commands to configure the match criteria for a class. Because you can configure a maximum of 64 class maps, a policy map cannot contain more than 64 class policies.

A single policy map can be attached to more than one interface concurrently. Except as noted, when you attempt to attach a policy map to an interface, the attempt is denied if the available bandwidth on the interface cannot accommodate the total bandwidth requested by class policies that make up the policy map. In this case, if the policy map is already attached to other interfaces, it is removed from them.

Whenever you modify class policy in an attached policy map, class-based weighted fair queueing (CBWFQ) is notified and the new classes are installed as part of the policy map in the CBWFQ system.



#### Note

Policy-map installation via subscriber-profile is not supported. If you configure an unsupported policy map and there are a large number of sessions, then an equally large number of messages print on the console. For example, if there are 32,000 sessions, then 32,000 messages print on the console at 9,600 baud.

### Examples

The following example creates a policy map called “policy1” and configures two class policies included in that policy map. The class policy called “class1” specifies policy for traffic that matches access control list (ACL) 136. The second class is the default class to which packets that do not satisfy configured match criteria are directed.

```
! The following commands create class-map class1 and define its match criteria:
```

```
class-map class1
  match access-group 136
```

```
! The following commands create the policy map, which is defined to contain policy
! specification for class1 and the default class:
```

```
policy-map policy1
```

```
class class1
  bandwidth 2000
  queue-limit 40
```

```
class class-default
  fair-queue 16
  queue-limit 20
```

The following example creates a policy map called “policy9” and configures three class policies to belong to that map. Of these classes, two specify policy for classes with class maps that specify match criteria based on either a numbered ACL or an interface name, and one specifies policy for the default class called “class-default” to which packets that do not satisfy configured match criteria are directed.

```
policy-map policy9

class acl136
  bandwidth 2000
  queue-limit 40

class ethernet101
  bandwidth 3000
  random-detect exponential-weighting-constant 10

class class-default
  fair-queue 10
  queue-limit 20
```

# preferred-path

Specifies the preferred path within an MPLS pseudowire-class where multiple paths exist. To remove a preferred path, use the **no** form of this command.

**preferred-path** {[interface] *tunnel tunnel*] | *peer peer*} **disable-fallback**

**no preferred-path** {[interface] *tunnel tunnel*] | *peer peer*} **disable-fallback**

## Syntax Description

|                         |                                                                        |
|-------------------------|------------------------------------------------------------------------|
| <b>interface</b>        | Specifies the preferred path using an output interface.                |
| <b>tunnel</b>           | Specifies a tunnel interface.                                          |
| <i>tunnel</i>           | The tunnel interface number.                                           |
| <b>peer</b>             | Specifies the preferred path using a peer host name or IP address.     |
| <i>peer</i>             | The peer host name or IP address.                                      |
| <b>disable-fallback</b> | Specifies that pseudowire class traffic cannot use an alternate route. |

## Command Default

This command is disabled by default.

## Command Modes

Pseudowire class configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.0(25)S   | This command was introduced.                                    |
| 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.   |
| 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.  |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Examples

The following example creates a pseudowire class called pw\_tun2, specifies MPLS encapsulation, and specifies a preferred path with fallback disabled.

```
Router# configure terminal
Router(config)# pseudowire-class pw_tun2
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# preferred-path peer 50.0.0.2 disable-fallback
```

# priority

To give priority to a class of traffic belonging to a policy map, use the **priority** command in policy-map class configuration mode. To remove a previously specified priority for a class, use the **no** form of this command.

**priority** { *bandwidth-kbps* | **percent** *percentage* } [*burst*]

**no priority** { *bandwidth-kbps* | **percent** *percentage* } [*burst*]

## Syntax Description

|                       |                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>bandwidth-kbps</i> | Specifies the guaranteed allowed bandwidth, in kbps, for the priority traffic. The amount of guaranteed bandwidth varies according to the interface and platform in use. Beyond the guaranteed bandwidth, the priority traffic is dropped in the event of congestion to ensure that the nonpriority traffic is not starved.                       |
| <b>percent</b>        | The amount of guaranteed bandwidth as specified a the percent of available bandwidth.                                                                                                                                                                                                                                                             |
| <i>percentage</i>     | Used in conjunction with the <b>percent</b> keyword, specifies the percentage of the total available bandwidth to be set aside for the priority class. The percentage can be a number from 1 to 100.                                                                                                                                              |
| <i>burst</i>          | (Optional) Specifies the burst size in bytes. The burst size configures the network to accommodate temporary bursts of traffic. The default burst value, which is computed as 200 milliseconds of traffic at the configured bandwidth rate, is used when the burst argument is not specified. The range of the burst is from 32 to 2000000 bytes. |

## Command Default

No priority is set.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release    | Modification                                                                                                                                                        |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(7)T   | This command was introduced.                                                                                                                                        |
| 12.0(5)XE5 | This command was introduced for the Versatile Interface Processor (VIP) as part of the Distributed Low Latency Queueing (Low Latency Queueing for the VIP) feature. |
| 12.0(9)S   | This command was introduced for the VIP as part of the Distributed Low Latency Queueing (Low Latency Queueing for the VIP) feature.                                 |
| 12.1(2)E   | The <i>burst</i> argument was added.                                                                                                                                |
| 12.1(3)T   | The <i>burst</i> argument was integrated in Release 12.1(3)T.                                                                                                       |
| 12.1(5)T   | This command was introduced for the VIP as part of the Distributed Low Latency Queueing (Low Latency Queueing for the VIP) feature.                                 |
| 12.2(2)T   | The <b>percent</b> keyword and the <i>percentage</i> argument were added.                                                                                           |

| Release                  | Modification                                                                                                                                                                      |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(28)SB               | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                                                                    |
| 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX                   | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers.                                                                                                                    |
| 12.4(20)MR               | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA              | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

### Usage Guidelines

This command configures low latency queueing (LLQ), providing strict priority queueing (PQ) for class-based weighted fair queueing (CBWFQ). Strict PQ allows delay-sensitive data such as voice to be dequeued and sent before packets in other queues are dequeued.

The **priority** command allows you to set up classes based on a variety of criteria (not just User Datagram Ports (UDP) ports) and assign priority to them, and is available for use on serial interfaces and ATM permanent virtual circuits (PVCs). A similar command, the **ip rtp priority** command, allows you to stipulate priority flows based only on UDP port numbers and is not available for ATM PVCs.

When the device is not congested, the priority class traffic is allowed to exceed its allocated bandwidth. When the device is congested, the priority class traffic above the allocated bandwidth is discarded.

The **bandwidth** and **priority** commands cannot be used in the same class, within the same policy map. These commands can be used together in the same policy map, however.

Within a policy map, you can give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is queued to the same, single, priority queue.

When the policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, the policy is removed from all interfaces to which it was successfully attached.

For more information on bandwidth allocation, see the chapter “Congestion Management Overview” in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

### Examples

The following example configures PQ with a guaranteed bandwidth of 50 kbps and a one-time allowable burst size of 60 bytes for the policy map called policy1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50 60
```

In the following example, 10 percent of the available bandwidth is reserved for the class called voice on interfaces to which the policy map called policy1 has been attached:

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority percent 10
```

| Related Commands | Command                           | Description                                                                                                                                                                         |
|------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>bandwidth</b>                  | Specifies or modifies the bandwidth allocated for a class belonging to a policy map.                                                                                                |
|                  | <b>ip rtp priority</b>            | Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports.                                                                       |
|                  | <b>ip rtp reserve</b>             | Reserves a special queue for a set of RTP packet flows belonging to a range of UDP destination ports.                                                                               |
|                  | <b>max-reserved-bandwidth</b>     | Changes the percent of interface bandwidth allocated for CBWFQ, LLQ, and IP RTP Priority.                                                                                           |
|                  | <b>show interfaces fair-queue</b> | Displays information and statistics about WFQ for a VIP-based interface.                                                                                                            |
|                  | <b>show policy-map</b>            | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.                                                           |
|                  | <b>show policy-map interface</b>  | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |
|                  | <b>show queue</b>                 | Displays the contents of packets inside a queue for a particular interface or VC.                                                                                                   |



## protocol (ATM)

To configure a static map for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), or virtual circuit (VC) class or to enable Inverse Address Resolution Protocol (ARP) or Inverse ARP broadcasts on an ATM PVC, use the **protocol** command in the appropriate mode. To remove a static map or disable Inverse ARP, use the **no** form of this command.

```
protocol protocol [protocol-address [virtual-template] | inarp] [[no] broadcast |  
disable-check-subnet | [no] enable-check-subnet]
```

```
no protocol protocol [protocol-address [virtual-template] | inarp] [[no] broadcast |  
disable-check-subnet | [no] enable-check-subnet]
```

### Syntax Description

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>protocol</i>         | Choose one of the following values: <ul style="list-style-type: none"> <li>• <b>arp</b>—IP ARP</li> <li>• <b>bridge</b>—bridging</li> <li>• <b>cdp</b>—Cisco Discovery Protocol</li> <li>• <b>clns</b>—ISO Connectionless Network Service (CLNS)</li> <li>• <b>clns_es</b>—ISO CLNS end system</li> <li>• <b>clns_is</b>—ISO CLNS intermediate system</li> <li>• <b>cmns</b>—ISO CMNS</li> <li>• <b>compressedtcp</b>—Compressed TCP</li> <li>• <b>ip</b>—IP</li> <li>• <b>ipv6</b>—IPV6</li> <li>• <b>llc2</b>—llc2</li> <li>• <b>pad</b>—packet assembler/disassembler (PAD) links</li> <li>• <b>ppp</b>—Point-to-Point Protocol carried on the VC</li> <li>• <b>pppoe</b>—PPP over Ethernet</li> <li>• <b>pppovlan</b>—PPPoE over vlan</li> <li>• <b>rsrb</b>—remote source-route bridging</li> <li>• <b>snapshot</b>—snapshot routing support</li> </ul> |
| <i>protocol-address</i> | Destination address that is being mapped to a PVC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>virtual-template</b> | (Optional) Specifies parameters that the point-to-point protocol over ATM (PPPoA) sessions use.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                         | <b>Note</b> This keyword is valid only for the PPP protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|                             |                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>inarp</b>                | Enables Inverse ARP on an ATM PVC. If you specify a protocol address instead of <b>inarp</b> , Inverse ARP is automatically disabled for that protocol.                                                                                                                                                                   |
| <b>[no] broadcast</b>       | (Optional) Indicates that this map entry is used when the corresponding protocol sends broadcast packets to the interface. Pseudobroadcasting is supported. The <b>broadcast</b> keyword of the <b>protocol</b> command takes precedence if you previously configured the <b>broadcast</b> command on the ATM PVC or SVC. |
| <b>disable-check-subnet</b> | (Optional) Disables subnet checking for InARP.                                                                                                                                                                                                                                                                            |
| <b>enable-check-subnet</b>  | (Optional) Enables subnet checking for InARP.                                                                                                                                                                                                                                                                             |

Inverse ARP is enabled for IP if the protocol is running on the interface and no static map is configured. Subnet checking for InARP is disabled by default.

### Command Modes

Interface-ATM-VC configuration (for an ATM PVC or SVC)  
PVC-in-range configuration (for an individual PVC within a PVC range)  
PVC range configuration (for an ATM PVC range)  
VC-class configuration (for a VC class)

### Command History

| Release     | Modification                                                                                                                                                                              |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.3        | This command was introduced.                                                                                                                                                              |
| 12.1        | The <b>ppp</b> and <b>virtual-template</b> keywords were added.                                                                                                                           |
| 12.1(5)T    | The <b>ip</b> and <b>ipx</b> options were made available in PVC range and PVC-in-range configuration modes.                                                                               |
| 12.2(13)T   | The <b>apollo</b> , <b>vines</b> , and <b>xns</b> keywords were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems are no longer supported in the Cisco IOS software. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                           |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.         |
| 12.2SRE     | The <b>disable-check-subnet</b> and <b>enable-check-subnet</b> keywords were added.                                                                                                       |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                            |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                           |

### Usage Guidelines

#### Command Application

Use this command to perform either of the following tasks:

- Configure a static map for an ATM PVC, SVC, or VC class.
- Enable Inverse ARP or Inverse ARP broadcasts on an ATM PVC or PVC range by configuring Inverse ARP directly on the PVC, in the PVC range, or in a VC class (applies to IP protocol only).
- Enable the router to respond to an InARP request when the source IP address contained in the request is not in the subnet as the receiving sub-interface on which PVC is configured.

- Enable the router to accept InARP reply when the peer router's IP address is not in the same subnet as the receiving sub-interface on which the PVC is configured.
- Does not provide support for SVC, PVC, and SVC bundles.

PVC range and PVC-in-range configuration modes support only IP.

---

**Examples**

In the following example, the router creates a static map on a VC, indicates that 10.68.34.237 is connected to this VC, and sends ATM pseudobroadcasts:

```
protocol ip 10.68.34.237 broadcast
```

In the following example, the router removes a static map from a VC and restores the default behavior for Inverse ARP (refer to the “Defaults” section):

```
no protocol ip 10.68.34.237
```

In the following example, the VC carries PPP traffic and its associated parameters:

```
protocol ppp 10.68.34.237 virtual-template
```

# pseudowire-class

To specify the name of a Layer 2 pseudowire-class and enter pseudowire-class configuration mode, use the **pseudowire-class** command in global configuration mode. To remove a pseudowire class configuration, use the **no** form of this command.

**pseudowire-class** *pw-class-name*

**no pseudowire-class** *pw-class-name*

## Syntax Description

|                      |                                                                                                                                                                |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>pw-class-name</i> | The name of a Layer 2 pseudowire-class. If you want to configure more than one pseudowire class, define a class name using the <i>pw-class-name</i> parameter. |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Command Default

No pseudowire-class is defined.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                                |
|-------------|-----------------------------------------------------------------------------|
| 12.0(23)S   | This command was introduced.                                                |
| 12.3(2)T    | This command was integrated into Cisco IOS Release 12.3(2)T.                |
| 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.               |
| 12.2(27)SBC | Support for this command was integrated into Cisco IOS Release 12.2(27)SBC. |
| 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2.             |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.             |

## Usage Guidelines

The **pseudowire-class** command configures a pseudowire-class template that consists of configuration settings used by all attachment circuits bound to the class. A pseudowire-class includes the following configuration settings:

- Data encapsulation type
- Control protocol
- IP address of the local Layer 2 interface
- Type of service (ToS) value in IP headers

The local interface name for each pseudowire class configured between a pair of PE routers can be the same or different.

After entering the **pseudowire-class** command, the router switches to pseudowire-class configuration mode where PW settings can be configured.

---

**Examples**

The following example shows how to enter pseudowire-class configuration mode to configure a PW configuration template named “ether-pw”:

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# exit
Router(config)# exit
```

---

**Related Commands**

| Command           | Description                                                                                                       |
|-------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>pseudowire</b> | Binds an attachment circuit to a Layer 2 PW for an xconnect service.                                              |
| <b>xconnect</b>   | Binds an attachment circuit to an Layer 2 PW for an xconnect service and then enters xconnect configuration mode. |

# ptp announce

Sets interval and timeout values for PTP announcement packets.

**ptp announce interval** *interval-value* **timeout** *timeout-value*

**no ptp announce interval** *interval-value* **timeout** *timeout-value*

| Syntax Description | interval              | Specifies an interval for PTP announce messages.                                                                                                                                                                                                                                                                                                  |
|--------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <i>interval-value</i> | Specifies the interval for PTP announce messages. The intervals are set using log base 2 values, as follows: <ul style="list-style-type: none"> <li>• 4—1 packet every 16 seconds</li> <li>• 3—1 packet every 8 seconds</li> <li>• 2—1 packet every 4 seconds</li> <li>• 1—1 packet every 2 seconds</li> <li>• 0—1 packet every second</li> </ul> |
|                    | <b>timeout</b>        | Specifies a timeout for PTP announcement packets.                                                                                                                                                                                                                                                                                                 |
|                    | <i>timeout-value</i>  | Specifies the number of PTP announcement intervals before the session times out. Valid values are 2–10.                                                                                                                                                                                                                                           |

**Command Default** The default interval value is 1. The default timeout value is 3.

**Command Modes** Interface configuration

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(19)MR2 | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** The recommended interval value is –6.

**Examples** The following example shows how to configure a PTP announce interval:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp announce interval 3
Router(config-if)# exit
Router(config)# exit
```

| Related Commands | Command                    | Description                       |
|------------------|----------------------------|-----------------------------------|
|                  | <a href="#">ptp enable</a> | Enables PTP mode on an interface. |

# ptp clock-destination

Specifies the IP address of a clock destination. This command applies only when the router is in PTP master unicast mode.

**ptp clock-destination** *clock-ip-address*

**no ptp clock-destination** *clock-ip-address*

|                           |                                                                  |
|---------------------------|------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>clock-ip-address</i> The IP address of the clock destination. |
|---------------------------|------------------------------------------------------------------|

|                        |                              |
|------------------------|------------------------------|
| <b>Command Default</b> | There is no default setting. |
|------------------------|------------------------------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | Interface configuration |
|----------------------|-------------------------|

|                        |                |                                                                 |
|------------------------|----------------|-----------------------------------------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                             |
|                        | 12.4(19)MR2    | This command was introduced.                                    |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                                                                                                                                                                                                                                                       |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | If the router is set to ptp master unicast, you can only configure a single destination. If the router is set to ptp master unicast negotiation, you do not need to use this command as the router uses negotiation to determine the IP address of PTP slave devices. |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                                  |
|-----------------|------------------------------------------------------------------|
| <b>Examples</b> | The following example shows how to configure a PTP announcement: |
|-----------------|------------------------------------------------------------------|

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp clock-destination 192.168.1.2
Router(config-if)# exit
Router(config)# exit
```

|                         |                         |                                                         |
|-------------------------|-------------------------|---------------------------------------------------------|
| <b>Related Commands</b> | <b>Command</b>          | <b>Description</b>                                      |
|                         | <b>ptp enable</b>       | Enables PTP mode on an interface.                       |
|                         | <b>ptp master</b>       | Sets an interface in master clock mode for PTP clocking |
|                         | <b>ptp mode</b>         | Specifies the PTP mode.                                 |
|                         | <b>ptp clock-source</b> | Specifies a PTP clock source.                           |



# ptp clock-source

Specifies the IP address of the clock source. This command only applies when the router is in PTP slave mode.

**ptp clock-source** *clock-ip-address*

**no ptp clock-source** *clock-ip-address*

## Syntax Description

*clock-ip-address* IP address of the clock source.

## Command Default

The default setting is **no ptp clock-source**.

## Command Modes

Interface configuration

## Command History

| Release     | Modification                                         |
|-------------|------------------------------------------------------|
| 12.4(19)MR2 | This command was introduced.                         |
| 12.2(33)MRA | Support for hot standby master clock was introduced. |

## Usage Guidelines

When the router is in PTP unicast slave mode, you can enable a hot standby master clock by configuring two **ptp clock-source** statements. A hot standby master clock allows the MWR 2941 to measure recovered clock quality from two PTP master clocks and switch dynamically between them. The MWR 2941 switches to the standby master clock when there is a lock between the router and clocking device and the advertised clock quality is greater than the current master clock.



### Note

Hot standby master clocking is an alternative to best master clock and disables best master clock when it is enabled.

## Examples

The following example shows how to configure a PTP clock source:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp clock-source 192.168.1.1
Router(config-if)# exit
Router(config)# exit
```

## Related Commands

| Command           | Description                       |
|-------------------|-----------------------------------|
| <b>ptp enable</b> | Enables PTP mode on an interface. |
| <b>ptp mode</b>   | Specifies the PTP mode.           |

| Command                      | Description                                             |
|------------------------------|---------------------------------------------------------|
| <b>ptp slave</b>             | Sets an interface to slave clock mode for PTP clocking. |
| <b>ptp clock-destination</b> | Specifies a PTP clock destination.                      |

# ptp delay-req interval

Specifies the delay request interval, the time recommended to member devices to send delay request messages when an interface is in PTP master mode.

**ptp delay-req interval** [*interval-value*]

**no ptp delay-req interval** [*interval-value*]

| Syntax Description | interval              | Specifies an interval for PTP delay requests.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <i>interval-value</i> | Specifies the length of the interval for delay request messages. The intervals are set using log base 2 values, as follows:<br><br>4—1 packet every 16 seconds<br>3—1 packet every 8 seconds<br>2—1 packet every 4 seconds<br>1—1 packet every 2 seconds<br>0—1 packet every second<br>-1—1 packet every 1/2 second, or 2 packets per second<br>-2—1 packet every 1/4 second, or 4 packets per second<br>-3—1 packet every 1/8 second, or 8 packets per second<br>-4—1 packet every 1/16 seconds, or 16 packets per second.<br>-5—1 packet every 1/32 seconds, or 32 packets per second.<br>-6—1 packet every 1/64 seconds, or 64 packets per second.<br>The recommended value is -6. |

|                        |                                      |
|------------------------|--------------------------------------|
| <b>Command Default</b> | This command is disabled by default. |
|------------------------|--------------------------------------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | Interface configuration |
|----------------------|-------------------------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(20)MR  | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                       |
|-------------------------|---------------------------------------|
| <b>Usage Guidelines</b> | The recommended interval value is -6. |
|-------------------------|---------------------------------------|

Examples

The following example shows how to configure a PTP delay-req interval:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp delay-req interval -4
Router(config-if)# exit
Router(config)# exit
```

Related Commands

| Command                      | Description                                                                                       |
|------------------------------|---------------------------------------------------------------------------------------------------|
| <b>ptp delay-req unicast</b> | Configures the Cisco MWR 2941 to send unicast PTP delay request messages while in multicast mode. |

# ptp delay-req unicast

Configures the Cisco MWR 2941 to send unicast PTP delay request messages while in multicast mode. This command helps reduce unnecessary PTP delay request traffic.



## Note

The Cisco MWR 2941 only supports multicast routing for PTP redundancy. For more information, see the [“Configuring Pseudowire-based Clocking with Adaptive Clock Recovery”](#) section on page 4-45.

**ptp delay-req unicast { negotiation | no-negotiation }**

**no ptp delay-req unicast { negotiation | no-negotiation }**

## Syntax Description

|                       |                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unicast</b>        | Configures the Cisco MWR 2941 to send unicast PTP delay request messages while in multicast mode.                                                                                                                                                                                                                                                                                   |
| <b>negotiation</b>    | Specifies that the Cisco MWR 2941 use unicast negotiation to discover the PTP master clock by sending delay request messages to all devices specified as PTP clock sources in the local router configuration.                                                                                                                                                                       |
| <b>no-negotiation</b> | Disables unicast negotiation on the Cisco MWR 2941 in slave mode. If you disable unicast negotiation, ensure that the PTP master clock is configured with the slave IP address. The slave Cisco MWR 2941 obtains the PTP master IP address from Announce messages received from the PTP master clock. The Cisco MWR 2941 then sends delay request messages to the PTP master clock. |

## Command Default

This command is disabled by default.

## Command Modes

Interface configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(20)MR  | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

If the Cisco MWR 2941 is in PTP multicast slave mode using unicast delay request messages and is connected to another Cisco MWR 2941 as a master clock, ensure that the master clock is also configured to use unicast delay request messages.

## Examples

The following example shows how to configure PTP delay-req unicast:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp delay-req unicast negotiation
Router(config-if)# exit
Router(config)# exit
```

ptp delay-req unicast

| Related Commands | Command                                | Description                               |
|------------------|----------------------------------------|-------------------------------------------|
|                  | <a href="#">ptp delay-req interval</a> | Specifies the PTP delay request interval. |

# ptp domain

PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. Use this command to specify the PTP domain number that the router uses.

**ptp domain** *domain-number*

**no ptp domain** *domain-number*

## Syntax Description

|                      |                                                                                    |
|----------------------|------------------------------------------------------------------------------------|
| <i>domain-number</i> | PTP domain that the router applies to PTP traffic. Valid values are from 0 to 127. |
|----------------------|------------------------------------------------------------------------------------|

## Command Default

The default setting is **ptp domain 0**.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(19)MR2 | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Examples

The following example shows how to set the ptp domain:

```
Router# config t  
Router# ptp domain 88  
Router(config)# exit
```

## Related Commands

| Command           | Description                       |
|-------------------|-----------------------------------|
| <b>ptp enable</b> | Enables PTP mode on an interface. |
| <b>ptp mode</b>   | Specifies the PTP mode.           |

# ptp enable

Enables PTP clocking on an interface.

**ptp enable**

**no ptp enable**

**Syntax Description** This command has no arguments or keywords.

**Command Default** PTP is disabled by default.

**Command Modes** Interface configuration

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(19)MR2 | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** You can apply this command to multiple interfaces.

**Examples** The following example shows how to configure a PTP announcement:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp enable
Router(config-if)# exit
Router(config)# exit
```

| Related Commands | Command           | Description                                             |
|------------------|-------------------|---------------------------------------------------------|
|                  | <b>ptp master</b> | Sets an interface in master clock mode for PTP clocking |
|                  | <b>ptp mode</b>   | Specifies the PTP mode.                                 |
|                  | <b>ptp slave</b>  | Sets an interface to slave clock mode for PTP clocking. |



# ptp input

Enables PTP input clocking using the 1.544Mhz, 2.048Mhz, or 10Mhz timing interface or phase using the 1PPS or RS-422 interface.

**ptp input** {[10M | 2.048M | 1.544M]} {[1pps] | [1pps rs422]}

**no ptp input** {[10M | 2.048M | 1.544M]} {[1pps] | [1pps rs422]}

| Syntax Description |                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>10M</b>         | Specifies PTP input at 10 Mhz using the 10Mhz timing port.                                                                                                                                 |
| <b>2.048M</b>      | Specifies PTP input at 2.048 Mhz using the 10Mhz timing port.                                                                                                                              |
| <b>1.544M</b>      | Specifies PTP input at 1.544 Mhz using the 10Mhz timing port.                                                                                                                              |
| <b>1pps</b>        | (Optional) Configures the router to receive 1 pulse per second (1PPS) time of day messages using the RS422 port or 1PPS port. You can select 1PPS with or without selecting a timing port. |
| <b>1pps rs422</b>  | (Optional) Configures the router to receive 1 pulse per second (1PPS) time of day messages using the RS-422 port.                                                                          |

**Command Default** This command is disabled by default.

**Command Modes** Global configuration

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(20)MR  | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |
|                 | 12.2(33)MRB | The <b>1pps rs422</b> keyword was introduced.                   |

**Usage Guidelines** If you are using GPS to provide clock source to the router, configure this command in PTP master mode.

**Examples** The following examples show how to configure PTP input clocking:

```
Router# config t
Router(config)# ptp input 10M
Router(config)# network-clock-select 5 10M
Router(config)# exit

Router# config t
Router(config)# ptp input 1pps
Router(config)# exit
```

ptp input

**Related Commands**

| Command                     | Description                                           |
|-----------------------------|-------------------------------------------------------|
| <b>network-clock-select</b> | Specifies a network clock timing source and priority. |

# ptp master

Sets an interface in master clock mode for PTP clocking. To enable ordinary master clock mode, use the **ptp master** command in interface configuration mode. To disable this feature, use the **no** form of this command.



## Note

The Cisco MWR 2941 only supports multicast routing for PTP redundancy. For more information, see the [“Configuring Pseudowire-based Clocking with Adaptive Clock Recovery”](#) section on page 4-45.

**ptp master {multicast | unicast [negotiation]}**

**no ptp master {multicast | unicast [negotiation]}**

## Syntax Description

|                    |                                                                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>multicast</b>   | Sets the interface to use multicast mode for PTP clocking.                                                                                                                                                       |
| <b>unicast</b>     | Sets the interface to use unicast mode for PTP clock.                                                                                                                                                            |
|                    | <b>Note</b> If the router is set to <b>ptp master unicast</b> , you can only configure a single destination.                                                                                                     |
| <b>negotiation</b> | (Optional) Sets the interface to negotiate unicast mode for PTP clocking.                                                                                                                                        |
|                    | <b>Note</b> If the router is set to <b>ptp master unicast negotiation</b> , you do not need to configure PTP clock destinations as the router uses negotiation to determine the IP address of PTP slave devices. |

## Command Default

There is no default setting.

## Command Modes

Interface configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(19)MR2 | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

For unicast and unicast negotiation, you must configure the ip address of the remote slave using the **ptp clock-destination** command before enabling PTP.

## Examples

The following example shows how to enable ptp master multicast mode:

```
Router# config t
Router# interface Vlan10
Router(config-if)# ptp master multicast
Router(config-if)# exit
Router(config)# exit
```

| Related Commands | Command                      | Description                                                                            |
|------------------|------------------------------|----------------------------------------------------------------------------------------|
|                  | <b>ptp clock-destination</b> | Specifies the IP address of a clock destination when the router is in PTP master mode. |
|                  | <b>ptp enable</b>            | Enables PTP mode on an interface.                                                      |
|                  | <b>ptp mode</b>              | Specifies the PTP mode.                                                                |

# ptp min-timing-pkt-size

This command allows you to modify the default size of PTP timing packets; in some conditions, modifying the PTP packet size can improve clock recovery performance.

**ptp min-timing-pkt-size** *size*

**no ptp min-timing-pkt-size** *size*

## Syntax Description

|             |                                                                                                           |
|-------------|-----------------------------------------------------------------------------------------------------------|
| <i>size</i> | Specifies the minimum PTP timing packet size in bytes. Valid values are 86–1510. The default value is 86. |
|-------------|-----------------------------------------------------------------------------------------------------------|

## Command Default

The default timing packet size is 86 bytes.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(19)MR2 | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

This command is not part of the IEEE-2008 PTP standard.

## Examples

The following example shows how to enable ptp master multicast mode:

```
Router# config t
Router(config)# ptp min-timing-pkt-size 100
Router(config)# exit
```

## Related Commands

| Command                      | Description                                                                            |
|------------------------------|----------------------------------------------------------------------------------------|
| <b>ptp clock-destination</b> | Specifies the IP address of a clock destination when the router is in PTP master mode. |
| <b>ptp enable</b>            | Enables PTP mode on an interface.                                                      |
| <b>ptp mode</b>              | Specifies the PTP mode.                                                                |

# ptp mode

Specifies the PTP mode.

**ptp mode [ordinary]**

**no ptp mode [ordinary]**



## Note

The Cisco MWR 2941 does not currently support other PTP modes such as boundary or transport mode.

## Syntax Description

|                 |                                                      |
|-----------------|------------------------------------------------------|
| <b>ordinary</b> | Sets the interface to PTP clocking mode to ordinary. |
|-----------------|------------------------------------------------------|

## Command Default

The default setting is **ptp mode ordinary**.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(19)MR2 | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Examples

The following example shows how to enable ptp mode:

```
Router# config t
Router(config)# ptp mode ordinary
Router(config)# exit
```

## Related Commands

| Command           | Description                                             |
|-------------------|---------------------------------------------------------|
| <b>ptp enable</b> | Enables PTP mode on an interface.                       |
| <b>ptp master</b> | Sets an interface in master clock mode for PTP clocking |
| <b>ptp slave</b>  | Sets an interface to slave clock mode for PTP clocking. |

# ptp output

Enables PTP output clocking using the 1.544Mhz, 2.048Mhz, or 10Mhz timing interface or time of day messages using the 1PPS interface.

**ptp output** {{{10M | 2.048M | 1.544M} [1pps [offset *offset-value*] [pulse-width *pulse-amount* {ns | us | ms}]]} | 1pps [pulse-width *pulse-amount* {ns | us | ms}]}

**no ptp output** {{{10M | 2.048M | 1.544M} [1pps [pulse-width *pulse-amount* {ns | us | ms}]]} | 1pps [offset *offset-value*] [pulse-width *pulse-amount* {ns | us | ms}]}

| Syntax              | Description                                                                                                                                                                          |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>10M</b>          | Specifies PTP output using the 10Mhz timing interface.                                                                                                                               |
| <b>2.048M</b>       | Specifies PTP output using the 2.048Mhz timing interface.                                                                                                                            |
| <b>1.544M</b>       | Specifies PTP output using the 1.544Mhz timing interface.                                                                                                                            |
| <b>1pps</b>         | Configures the router to send 1 packet per second (1PPS) time of day messages using the RS422 port or 1PPS port. You can select 1PPS output with or without selecting a timing port. |
| <b>offset</b>       | (Optional) Specifies an offset in order to compensate for a known phase error such as network asymmetry.                                                                             |
| <i>offset-value</i> | Amount of offset in nanoseconds. Valid values are -500000000 to 500000000.                                                                                                           |
| <b>pulse-width</b>  | (Optional) Specifies a pulse width value.                                                                                                                                            |
| <i>pulse-amount</i> | Amount of the pulse width. Valid values are 1–4096.<br>For 1PPS output using the RS422 port, you must specify a value of at least 2ms.                                               |
| <b>ns</b>           | (Optional) Specifies a pulse width value in nanoseconds.                                                                                                                             |
| <b>us</b>           | (Optional) Specifies a pulse width value in microseconds.                                                                                                                            |
| <b>ms</b>           | (Optional) Specifies a pulse width value in milliseconds.                                                                                                                            |

**Command Default** This command is disabled by default.

**Command Modes** Global configuration

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(20)MR  | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** If you want to provide output frequency clock, configure this command in PTP slave mode.

---

**Examples**

The following example shows how to configure PTP output clocking:

```
Router# config t  
Router(config)# ptp output 10M 1pps pulse-width 1000 ms  
Router(config)# exit
```

---

**Related Commands**

| Command                     | Description                                           |
|-----------------------------|-------------------------------------------------------|
| <b>network-clock-select</b> | Specifies a network clock timing source and priority. |



# ptp priority1

Sets the preference level for a clock; slave devices use the priority1 value when selecting a master clock. The priority1 value is considered above all other clock attributes. Use the following commands to set the ptp priority1 value.

**ptp priority1** *priorityvalue*

**no ptp priority1** *priorityvalue*

## Syntax Description

|                      |                                                           |
|----------------------|-----------------------------------------------------------|
| <i>priorityvalue</i> | Valid values are from 0 to 255. The default value is 128. |
|----------------------|-----------------------------------------------------------|

## Command Default

The default value is 128.

## Command Modes

Interface configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(19)MR2 | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Examples

The following example shows how to enable ptp priority1 value:

```
Router# config t
Router# interface Vlan10
Router(config-if)# ptp priority1 128
Router(config-if)# exit
Router(config)# exit
```

## Related Commands

| Command              | Description                   |
|----------------------|-------------------------------|
| <b>ptp priority2</b> | Sets the PTP priority2 value. |

# ptp priority2

Sets a secondary preference level for a clock; slave devices use the priority2 value when selecting a master clock. The priority2 value is considered only when the router is unable to use priority2 and other clock attributes to select a clock. Use the following commands to set the ptp priority2 value.

**ptp priority2** *priorityvalue*

**no ptp priority2** *priorityvalue*

## Syntax Description

*priorityvalue* Valid values are from 0 to 255. The default value is 128.

## Command Default

The default value is 128.

## Command Modes

Interface configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(19)MR2 | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Examples

The following example shows how to configure the ptp priority2 value:

```
Router# config t
Router# interface Vlan10
Router(config-if)# ptp priority2 128
Router(config-if)# exit
Router(config)# exit
```

## Related Commands

| Command              | Description                   |
|----------------------|-------------------------------|
| <b>ptp priority1</b> | Sets the PTP priority1 value. |

# ptp slave

Sets an interface to slave clock mode for PTP clocking. To enable ordinary slave clock mode, use the **ptp slave** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**Note**

The Cisco MWR 2941 only supports multicast routing for PTP redundancy. For more information, see the [“Configuring Pseudowire-based Clocking with Adaptive Clock Recovery”](#) section on page 4-45.

**ptp slave {multicast | unicast [negotiation]} [hybrid]**

**no ptp slave {multicast | unicast [negotiation]} [hybrid]**

**Syntax Description**

|                    |                                                                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>multicast</b>   | Sets the interface to use multicast mode for PTP clocking.                                                                                                                                                                                                                |
| <b>unicast</b>     | Sets the interface to use unicast mode for PTP clocking.                                                                                                                                                                                                                  |
| <b>negotiation</b> | (Optional) Sets the interface to negotiate unicast mode for PTP clocking.                                                                                                                                                                                                 |
| <b>hybrid</b>      | (Optional) Enables hybrid clocking mode, in which the Cisco MWR 2941 uses clock frequency obtained from the synchronous Ethernet port while using phase (ToD or 1PPS) obtained using PTP. You must enable synchronous Ethernet network clocking to configure hybrid mode. |

**Command Default**

There is no default setting.

**Command Modes**

Interface configuration

**Command History**

| Release     | Modification                                    |
|-------------|-------------------------------------------------|
| 12.4(19)MR2 | This command was introduced.                    |
| 12.2(33)MRA | Added parameter to enable hybrid clocking mode. |

**Usage Guidelines**

You must configure the IP address of the remote timing device before enabling PTP.

To configure hybrid mode, ensure that you have selected a synchronous Ethernet timing source using the **network-clock-select** command. You cannot configure hybrid mode if **network-clock-select** is configured for packet timing.

**Examples**

The following example shows how to enable ptp slave multicast mode:

```
Router# config t
Router# interface Vlan10
Router(config-if)# ptp slave multicast
Router(config-if)# exit
Router(config)# exit
```

| Related Commands | Command                 | Description                                                                                                   |
|------------------|-------------------------|---------------------------------------------------------------------------------------------------------------|
|                  | <b>ptp clock-source</b> | Specifies the IP address of the clock source. This command only applies when the router is in PTP slave mode. |
|                  | <b>ptp enable</b>       | Enables PTP mode on an interface.                                                                             |
|                  | <b>ptp mode</b>         | Specifies the PTP mode.                                                                                       |

# ptp sync interval

Specifies the interval used to send PTP sync messages.

**ptp sync interval** *interval-value*

**no ptp sync interval** *interval-value*

| Syntax Description | interval              | Specifies an interval for sending PTP sync packets.                                                                       |
|--------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------|
|                    | <i>interval-value</i> | Specifies the interval at which the router sends sync packets. The intervals are set using log base 2 values, as follows: |
|                    |                       | 4—1 packet every 16 seconds                                                                                               |
|                    |                       | 3—1 packet every 8 seconds                                                                                                |
|                    |                       | 2—1 packet every 4 seconds                                                                                                |
|                    |                       | 1—1 packet every 2 seconds                                                                                                |
|                    |                       | 0—1 packet every second                                                                                                   |
|                    |                       | -1—1 packet every 1/2 second, or 2 packets per second                                                                     |
|                    |                       | -2—1 packet every 1/4 second, or 4 packets per second                                                                     |
|                    |                       | -3—1 packet every 1/8 second, or 8 packets per second                                                                     |
|                    |                       | -4—1 packet every 1/16 seconds, or 16 packets per second.                                                                 |
|                    |                       | -5—1 packet every 1/32 seconds, or 32 packets per second.                                                                 |
|                    |                       | -6—1 packet every 1/64 seconds, or 64 packets per second.                                                                 |
|                    |                       | The recommended value is -6.                                                                                              |

**Command Default** There is no default setting.

**Command Modes** Interface configuration

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(19)MR2 | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Examples** The following example shows how to configure a PTP sync interval.

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp sync interval -4
Router(config-if)# exit
Router(config)# exit
```

ptp sync interval

| Related Commands | Command                 | Description                                                                                                   |
|------------------|-------------------------|---------------------------------------------------------------------------------------------------------------|
|                  | <b>ptp clock-source</b> | Specifies the IP address of the clock source. This command only applies when the router is in PTP slave mode. |
|                  | <b>ptp enable</b>       | Enables PTP mode on an interface.                                                                             |
|                  | <b>ptp mode</b>         | Specifies the PTP mode.                                                                                       |

# ptp tod

Configures the time of day message format used by the 1PPS interface.

**ptp tod** {iso8601 | ubx | nmea | cisco | ntp} *delay-amount*

**no ptp tod** {iso8601 | ubx | nmea | cisco | ntp} *delay-amount*

## Syntax Description

|                     |                                                                                                        |
|---------------------|--------------------------------------------------------------------------------------------------------|
| <b>iso8601</b>      | Specifies ISO 8601 time of day format.                                                                 |
| <b>ubx</b>          | Specifies UBX time of day format.                                                                      |
| <b>nmea</b>         | Specifies NMEA time of day format.                                                                     |
| <b>cisco</b>        | Specifies Cisco time of day format.                                                                    |
| <b>ntp</b>          | Specifies NTP time of day format.                                                                      |
| <i>delay-amount</i> | Delay in milliseconds between the 1PPS message and the time of day message. Valid values are 1 to 999. |

## Command Default

The default configuration is **ptp tod iso8601**.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(20)MR  | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

This command applies only to the Cisco MWR 2941-DC-A; it does not apply to the Cisco MWR 2941-DC.

## Examples

The following example shows how to configure a PTP announcement interval.

```
Router# config t
Router(config)# ptp tod ubx 100
Router(config)# exit
```

## Related Commands

| Command                | Description                                                         |
|------------------------|---------------------------------------------------------------------|
| <b>ptp enable</b>      | Enables PTP mode on an interface.                                   |
| <b>ptp mode</b>        | Specifies the PTP mode.                                             |
| <b>ptp 1pps enable</b> | Configures the router to send or receive 1PPS time of day messages. |

## ptp two-steps

The default PTP synchronization consists of a one-step handshake between the PTP master and slave devices. The **ptp two-steps** command configures the master clock to send a follow-up message containing the timestamp of the original synchronization message. This command is useful when the Cisco MWR 2941 is acting as the PTP master and is connected to a slave device that requires a two-step handshake.

**ptp two-steps**

**no ptp two-steps**



### Note

When configured as a PTP slave device, the Cisco MWR 2941 can use a one- or two-step handshake.

### Command Default

This command is disabled by default.

### Command Modes

Global configuration

### Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(20)MR  | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

### Examples

The following example shows how to configure a PTP two-step handshake:

```
Router# config t
Router(config-if)# ptp two-steps
Router(config)# exit
```

### Related Commands

| Command                  | Description                                                                     |
|--------------------------|---------------------------------------------------------------------------------|
| <b>ptp sync interval</b> | Defines the interval that the router uses to send PTP synchronization messages. |



# ptp update-calendar

Configures the router to periodically update the system calendar to match the PTP clock.

**ptp update-calendar**

**no ptp update-calendar**

|                           |                                            |
|---------------------------|--------------------------------------------|
| <b>Syntax Description</b> | This command has no arguments or keywords. |
|---------------------------|--------------------------------------------|

|                        |                                      |
|------------------------|--------------------------------------|
| <b>Command Default</b> | This command is disabled by default. |
|------------------------|--------------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(20)MR  | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |
|                 |             |                                                                 |

|                 |                                                                           |
|-----------------|---------------------------------------------------------------------------|
| <b>Examples</b> | The following example shows how to configure a PTP announcement interval. |
|-----------------|---------------------------------------------------------------------------|

```
Router# config t
Router(config)# ptp update-calendar
Router(config)# exit
```

| Related Commands | Command                      | Description                                                   |
|------------------|------------------------------|---------------------------------------------------------------|
|                  | <b>clock update-calendar</b> | Manually updates the system time to match the PTP clock time. |

# pw-pvc

To configure PVC mapping or rewrite the PW configured for a PVC, use the **pw-pvc** command. This command specifies the PW-side VPI/VCI value to be used inside the PW packet payload in sending and receiving PW packets for a specified PVC.

**pw-pvc** *pw-vpi/pw-vci*

| Syntax Description | <i>pw-vpi</i> | Pseudowire-side vpi value |
|--------------------|---------------|---------------------------|
|                    | <i>pw-vci</i> | Pseudowire-side vci value |

**Command Default** The PW-side VPI/VCI value is the same as the attachment circuit-side VPI/VCI value.

**Command Modes** l2transport VC

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Examples** The following example shows how to use the **pw-pvc** command:

```
Router# config t
Router(config-if)# pvc 0/40 l2transport
Router(config-if-atm-l2trans-pvc)# encapsulation aa10
Router(config-if-atm-l2trans-pvc)# pw-pvc 1/40
Router(config-if-atm-l2trans-pvc)# xconnect 1.1.1.1 40 encapsulation mpls
Router(config-if-atm-l2trans-pvc-xconn)# exit
Router(config-if-atm-l2trans-pvc)# exit
Router(config-if)# exit
Router(config)# exit
```

| Related Commands | Command         | Description                                                                      |
|------------------|-----------------|----------------------------------------------------------------------------------|
|                  | <b>xconnect</b> | Binds an attachment circuit to a PW in one of the supported configuration modes. |

# ql-enabled rep segment

Specifies the REP segment used for synchronous Ethernet clock selection. For more information about clock selection, see the [“Configuring Network Clock Quality Selection Using REP”](#) section on page 4-47.

**ql-enabled rep segment** *segment-id*

**no ql-enabled rep segment** *segment-id*

## Syntax Description

|                   |                                   |
|-------------------|-----------------------------------|
| <b>segment</b>    | Specifies a REP segment.          |
| <i>segment-id</i> | REP segment ID of the REP segment |

## Command Default

There is no default setting.

## Command Modes

Global configuration

## Command History

| Release     | Modification                 |
|-------------|------------------------------|
| 12.2(33)MRA | This command was introduced. |

## Usage Guidelines

This command requires that you specify a synchronous Ethernet clock source.

## Examples

The following example shows how to use the **pw-pvc** command:

```
Router# config t
Router(config)# ql-enabled rep segment 5
Router(config)# exit
```

## Related Commands

| Command            | Description                                                                     |
|--------------------|---------------------------------------------------------------------------------|
| <b>rep segment</b> | Enables Resilient Ethernet Protocol (REP) on an interface assigns a segment ID. |

# queue-limit

To specify or modify the queue limit (size) for a class in bytes, milliseconds (ms), or packets use the **queue-limit** command in policy-map class configuration mode. To remove the queue limit from a class, use the **no** form of this command.

**queue-limit** *queue-limit-size* [**bytes** | **ms** | **packets**]

**no queue-limit**

## Syntax Description

|                         |                                                                                                                                                                                                                                                                                          |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>queue-limit-size</i> | Maximum size of the queue. The maximum varies according to the optional unit of measure keyword specified ( <b>bytes</b> , <b>ms</b> , or <b>packets</b> ).                                                                                                                              |
|                         | <b>Note</b> If an optional unit of measure is not indicated, the default unit of measure is packets.                                                                                                                                                                                     |
| <b>bytes</b>            | (Optional) Indicates that the unit of measure is bytes. Valid range for bytes is a number from 1 to 8192000.                                                                                                                                                                             |
| <b>ms</b>               | (Optional) Indicates that the unit of measure is milliseconds. Valid range for milliseconds is a number from 1 to 3400.                                                                                                                                                                  |
| <b>packets</b>          | (Optional) Indicates that the unit of measure is packets. Valid range for packets is a number from 1 to 32768 but can also vary by platform and release as follows:<br><br><b>Note</b> The maximum value of the <i>queue-limit-size</i> parameter is 60 packets for Ethernet interfaces. |

## Command Default

The default behavior of the **queue-limit** command for class queues with and without weighted random early detection (WRED) is as follows:

- Class queues with WRED—The router uses the default queue limit of two times the largest WRED maximum threshold value, rounded to the nearest power of 2.
- Priority queues and class queues without WRED—The router has buffers for up to 50 ms of 256-byte packets at line rate, but not fewer than 32 packets.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release    | Modification                                                                                                               |
|------------|----------------------------------------------------------------------------------------------------------------------------|
| 12.0(5)T   | This command was introduced.                                                                                               |
| 12.0(5)XE  | This command was integrated into Cisco IOS Release 12.0(5)XE. Support for VIP-enabled Cisco 7500 series routers was added. |
| 12.0(17)SL | This command was implemented on the Cisco 10000 series router.                                                             |
| 12.1(5)T   | This command was implemented on the VIP-enabled Cisco 7500 series routers.                                                 |
| 12.2(16)BX | This command was introduced on the ESR-PRE2.                                                                               |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                             |

| Release                  | Modification                                                                                                                                                                                                                                                                |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                                                                                                             |
| 12.3(7)XI                | This command was integrated into Cisco IOS Release 12.3(7)XI.                                                                                                                                                                                                               |
| 12.2SX                   | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.                                                                                           |
| 12.4(20)T                | The following argument/keyword combinations were added: <ul style="list-style-type: none"> <li><i>queue-limit-size</i> <b>bytes</b></li> <li><i>queue-limit-size</i> <b>ms</b></li> <li><i>queue-limit-size</i> <b>packets</b></li> </ul>                                   |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers.                                                                                                                                                                                                              |
| 12.4(20)MR               | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                                                                                                              |
| 12.2(33)MRA              | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                                                                                                             |
| 12.2(333)MRB3            | The following modifications were introduced: <ul style="list-style-type: none"> <li>Support for the <b>queue-limit</b> command on Ethernet interfaces</li> <li>The maximum value of the <i>queue-limit-size</i> parameter is 60 packets for Ethernet interfaces.</li> </ul> |

## Usage Guidelines

### Weighted Fair Queueing

Weighted fair queueing (WFQ) creates a queue for every class for which a class map is defined. Packets that satisfy the match criterion for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queueing process. When the maximum packet threshold that you defined for the class is reached, enqueueing of any further packets to the class queue causes tail drop or, if WRED is configured for the class policy, packet drop to take effect.

### Overriding Queue Limits Set by the bandwidth Command

Use the **bandwidth** command with the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) to specify the bandwidth for a particular class. When used with MQC, the **bandwidth** command has a default queue limit for the class. This queue limit can be modified using the **queue-limit** command, thereby overriding the default set by the **bandwidth** command.



#### Note

Using the **queue-limit** command to modify the default queue limit is especially important for higher-speed interfaces, in order to meet the minimum bandwidth guarantees required by the interface.

## Examples

The following example configures a policy map called policy11. The policy11 policy map contains a class called acl203. The policy map for this class is configured so that the queue reserved for the class has a maximum queue size of 40 packets.

```
Router(config)# policy-map policy11
Router(config-pmap)# class acl203
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40 packets
```

| Related Commands | Command                    | Description                                                                                                                                                                   |
|------------------|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>bandwidth</b>           | Specifies the maximum aggregate bandwidth for H.323 traffic and verifies the available bandwidth of the destination gatekeeper.                                               |
|                  | <b>class (policy-map)</b>  | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |
|                  | <b>class class-default</b> | Specifies the default traffic class whose bandwidth is to be configured or modified.                                                                                          |
|                  | <b>policy-map</b>          | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                  |

# random-detect

To enable Weighted Random Early Detection (WRED) or distributed WRED (DWRED) on an interface, use the **random-detect** command in interface configuration mode. To configure WRED for a class in a policy map, use the **random-detect** command in policy-map class configuration mode. To disable WRED or DWRED, use the **no** form of this command.

**random-detect** [**dscp-based** | **precedence-based**]

**no random-detect**

|                           |                         |                                                                                                                                                    |
|---------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>dscp-based</b>       | (Optional) Specifies that WRED is to use the differentiated services code point (DSCP) value when it calculates the drop probability for a packet. |
|                           | <b>precedence-based</b> | (Optional) Specifies that WRED is to use the IP Precedence value when it calculates the drop probability for a packet.                             |

**Command Default** WRED and DWRED are disabled by default.

**Command Modes** Interface configuration when used on an interface (config-if)  
Policy-map class configuration when used in a policy map (config-pmap-c)

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                                                                                                                                                             |
|------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | 11.1CC         | This command was introduced.                                                                                                                                                                                                                                                    |
|                        | 12.1(5)T       | This command was integrated into Cisco IOS Release 12.1(5)T. Arguments were added to support Differentiated Services (DiffServ) and Assured Forwarding (AF) Per Hop Behavior (PHB).                                                                                             |
|                        | 12.1(5a)E      | This command was integrated into Cisco IOS Release 12.1(5a)E in policy map class configuration mode only.<br><br>This command was implemented on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers and Catalyst 6000 family switches with a FlexWAN module. |
|                        | 12.0(15)S      | This command was integrated into Cisco IOS Release 12.0(15)S in policy-map class configuration mode only.                                                                                                                                                                       |
|                        | 12.2(14)S      | This command was integrated into Cisco IOS Release 12.2(14)S.                                                                                                                                                                                                                   |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                                                                                                                 |
|                        | 12.2SX         | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.                                                                                               |
|                        | 12.4(20)T      | Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).                                                                                                                                      |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                                                                                                                  |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                                                                                                                 |

**Usage Guidelines****Keywords**

If you choose not to use either the **dscp-based** or the **precedence-based** keywords, WRED uses the IP Precedence value (the default method) to calculate the drop probability for the packet.

**Availability**

The **random-detect** command is not available at the interface level for Cisco IOS Releases 12.1E or 12.0S. The **random-detect** command is available in policy-map class configuration mode only for Cisco IOS Releases 12.1E, 12.0S, and later.

**WRED Functionality**

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP). WRED and DWRED are most useful with protocols like Transport Control Protocol (TCP) that respond to dropped packets by decreasing the transmission rate.

The router automatically determines parameters to use in the WRED calculations. To change these parameters, use the **random-detect precedence** command.

**WRED in a Policy Map**

You can configure WRED as part of the policy map for a standard class or the default class. The WRED **random-detect** command and the weighted fair queueing (WFQ) **queue-limit** command are mutually exclusive. If you configure WRED, its packet drop capability is used to manage the queue when packets exceeding the configured maximum count are enqueued. If you configure the WFQ **queue-limit** command, tail drop is used.

To configure a policy map and create class policies, use the **policy-map** and **class** (policy-map) commands. When creating a class within a policy map, you can use the **random-detect** command with either of the following commands:

- **bandwidth** (policy-map class)
- **fair-queue** (class-default)—for the default class only

**Note**

If you use WRED packet drop instead of tail drop for one or more classes in a policy map, you must ensure that WRED is not configured on the interface to which you attach that policy map.

**Note**

DWRED is not supported for classes in a policy map.

**Two Methods for Calculating the Drop Probability of a Packet**

This command includes two optional keywords, **dscp-based** and **precedence-based**, that determine the method WRED uses to calculate the drop probability of a packet.

Note the following points when deciding which method to instruct WRED to use:

- With the **dscp-based** keyword, WRED uses the DSCP value (that is, the first six bits of the IP type of service (ToS) byte) to calculate the drop probability.
- With the **precedence-based** keyword, WRED uses the IP Precedence value to calculate the drop probability.
- The **dscp-based** and **precedence-based** keywords are mutually exclusive.
- If neither argument is specified, WRED uses the IP Precedence value to calculate the drop probability (the default method).



**Examples**

The following example configures the policy map called policy1 to contain policy specification for the class called class1. During times of congestion, WRED packet drop is used instead of tail drop.

```
! The following commands create the class map called class1:
class-map class1
match input-interface gigabitethernet0/1
```

```
! The following commands define policy1 to contain policy specification for class1:
policy-map policy1
class class1
bandwidth 1000
random-detect
```

The following example enables WRED to use the DSCP value 8. The minimum threshold for the DSCP value 8 is 24 and the maximum threshold is 40. This configuration was performed at the interface level.

```
Router(config)# interface serial10/0
Router(config-if)# random-detect dscp-based
Router(config-if)# random-detect dscp 8 24 40
```

The following example enables WRED to use the DSCP value 8 for class c1. The minimum threshold for DSCP value 8 is 24 and the maximum threshold is 40. The last line attaches the service policy to the output interface or virtual circuit (VC) p1.

```
Router(config-if)# class-map c1
Router(config-cmap)# match access-group 101
Router(config-if)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# bandwidth 48
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp 8 24 40
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial10/0
Router(config-if)# service-policy output p1
```

**Related Commands**

| Command                                             | Description                                                                                     |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------|
| <b>random-detect dscp</b>                           | Changes the minimum and maximum packet thresholds for the DSCP value.                           |
| <b>random-detect exponential-weighting-constant</b> | Configures the WRED and DWRED exponential weight factor for the average queue size calculation. |
| <b>random-detect flow</b>                           | Enables flow-based WRED.                                                                        |
| <b>random-detect precedence</b>                     | Configures WRED and DWRED parameters for a particular IP Precedence.                            |
| <b>show interfaces</b>                              | Displays statistics for all interfaces configured on the router or access server.               |
| <b>show queueing</b>                                | Lists all or selected configured queueing strategies.                                           |
| <b>show tech-support rsvp</b>                       | Generates a report of all RSVP-related information.                                             |

# random-detect atm-clp-based

To enable weighted random early detection (WRED) on the basis of the ATM cell loss priority (CLP) of a packet, use the **random-detect atm-clp-based** command in policy-map class configuration mode. To disable WRED, use the **no** form of this command.

**random-detect atm-clp-based** *clp-value*

**no random-detect atm-clp-based**

|                           |                                                      |
|---------------------------|------------------------------------------------------|
| <b>Syntax Description</b> | <i>clp-value</i> CLP value. Valid values are 0 or 1. |
|---------------------------|------------------------------------------------------|

|                        |                                                                                                                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Command Default</b> | When WRED is configured, the default minimum and maximum thresholds are determined on the basis of output buffering capacity and the transmission speed for the interface.<br>The default maximum probability denominator is 10. |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                      |                                                |
|----------------------|------------------------------------------------|
| <b>Command Modes</b> | Policy-map class configuration (config-pmap-c) |
|----------------------|------------------------------------------------|

| Command History | Release     | Modification                                                                                                                               |
|-----------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.0(28)S   | This command was introduced.                                                                                                               |
|                 | 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                             |
|                 | 12.2(33)SB  | This command was introduced on the PRE3 and PRE4 for the Cisco 10000 series router.                                                        |
|                 | 12.4(20)T   | Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC). |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                             |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                            |

|                         |                                                                                                                                                                                                                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | You cannot use the <b>random-detect atm-clp-based</b> command with the <b>random-detect cos-based</b> command in the same HQF configuration. You must use the <b>no random-detect cos-based</b> command to disable it before you configure the <b>random-detect atm-clp-based</b> command. |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                                                                                                                                                                             |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | In the following example, WRED is configured on the basis of the ATM CLP. In this configuration, the <b>random-detect atm-clp-based</b> command has been configured and an ATM CLP of 1 has been specified. |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
Router> enable
Router# configure terminal
Router(config)# policy-map policymap1
Router(config-pmap)# class class1
Router(config-pmap-c)# random-detect atm-clp-based 1
Router(config-pmap-c)# end
```

| Related Commands | Command                          | Description                                                                                                                                                                         |
|------------------|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>random-detect clp</b>         | Specifies the ATM CLP value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED.                                        |
|                  | <b>random-detect cos</b>         | Specifies the CoS value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED.                                            |
|                  | <b>random-detect cos-based</b>   | Enables WRED on the basis of the CoS value of a packet.                                                                                                                             |
|                  | <b>show policy-map</b>           | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.                                                           |
|                  | <b>show policy-map interface</b> | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# random-detect cos-based

To enable weighted random early detection (WRED) on the basis of the class of service (CoS) value of a packet, use the **random-detect cos-based** command in policy-map class configuration mode. To disable WRED, use the **no** form of this command.

**random-detect cos-based** *cos-value*

**no random-detect cos-based**

|                           |                  |                                              |
|---------------------------|------------------|----------------------------------------------|
| <b>Syntax Description</b> | <i>cos-value</i> | Specific IEEE 802.1Q CoS values from 0 to 7. |
|---------------------------|------------------|----------------------------------------------|

|                        |                                                                                                                                                                                                                                      |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Command Default</b> | When WRED is configured, the default minimum and maximum thresholds are determined on the basis of output buffering capacity and the transmission speed for the interface.<br><br>The default maximum probability denominator is 10. |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                      |                                                |
|----------------------|------------------------------------------------|
| <b>Command Modes</b> | Policy-map class configuration (config-pmap-c) |
|----------------------|------------------------------------------------|

|                        |                |                                                                                                                                            |
|------------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                        |
|                        | 12.0(28)S      | This command was introduced.                                                                                                               |
|                        | 12.2(28)SB     | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                             |
|                        | 12.4(20)T      | Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC). |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                             |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                            |

|                         |                                                                                                                                                                                                                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | You cannot use the <b>random-detect cos-based</b> command with the <b>random-detect atm-clp-based</b> command in the same HQF configuration. You must use the <b>no random-detect atm-clp-based</b> command to disable it before you configure the <b>random-detect cos-based</b> command. |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                                                                                                                                                                            |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | In the following example, WRED is configured on the basis of the CoS value. In this configuration, the <b>random-detect cos-based</b> command has been configured and a CoS value of 2 has been specified. |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
Router> enable
Router# configure terminal
Router(config)# policy-map policymap1
Router(config-pmap)# class class1
Router(config-pmap-c)# random-detect cos-based 2
Router(config-pmap-c)# end
```

| Related Commands | Command                            | Description                                                                                                                                                                         |
|------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>random-detect atm-clp-based</b> | Enables WRED on the basis of the ATM CLP of a packet.                                                                                                                               |
|                  | <b>random-detect clp</b>           | Specifies the ATM CLP value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED.                                        |
|                  | <b>random-detect cos</b>           | Specifies the CoS value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED.                                            |
|                  | <b>show policy-map</b>             | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.                                                           |
|                  | <b>show policy-map interface</b>   | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# random-detect discard-class

To configure the weighted random early detection (WRED) parameters for a discard-class value for a class policy in a policy map, use the **random-detect discard-class** command in QoS policy-map class configuration mode. To disable the discard-class values, use the **no** form of this command.

**random-detect discard-class** *value min-threshold max-threshold max-probability-denominator*

**no random-detect discard-class** *value min-threshold max-threshold max-probability-denominator*

| Syntax Description                 |  |                                                                                                                                                                                                                                                                            |
|------------------------------------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>value</i>                       |  | Discard class. This is a number that identifies the drop eligibility of a packet. Valid values are 0 to 7.                                                                                                                                                                 |
| <i>min-threshold</i>               |  | Specifies the minimum number of packets allowed in the queue. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified DSCP, IP precedence, or discard-class value. Valid minimum threshold values are 1 to 16384. |
| <i>max-threshold</i>               |  | Specifies the maximum number of packets allowed in the queue. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP, IP precedence, or discard-class value. Valid maximum threshold values are 1 to 16384.           |
| <i>max-probability-denominator</i> |  | Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. Valid values are 1 to 65535.   |

| Command Default |                                                                                                                                                         |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | For all precedence levels, the <i>max-probability-denominator</i> default is 10 packets; 1 out of every 10 packets is dropped at the maximum threshold. |

| Command Modes |                                    |
|---------------|------------------------------------|
|               | QoS policy-map class configuration |

| Command History | Release     | Modification                                                                                                    |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------|
|                 | 12.0(3)T    | This command was introduced.                                                                                    |
|                 | 12.2(13)T   | This command was integrated into Cisco IOS Release 12.2(13)T.                                                   |
|                 | 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                  |
|                 | 12.2(31)SB  | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router. |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                  |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                 |

**Usage Guidelines**

When you configure the **random-detect discard-class** command on an interface, packets are given preferential treatment based on the discard class of the packet. Use the **random-detect discard-class** command to adjust the discard class for different discard-class values.

**Examples**

The following example shows how to configure discard class 2 to randomly drop packets when the average queue reaches the minimum threshold of 100 packets and 1 in 10 packets are dropped when the average queue is at the maximum threshold of 200 packets:

```
policy-map set-MPLS-PHB
class IP-AF11
  bandwidth percent 40
  random-detect discard-class-based
  random-detect-discard-class 2 100 200 10
```

**Related Commands**

| Command                                             | Description                                                                                                                                                                                  |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bandwidth (policy-map class)</b>                 | Specifies or modifies the bandwidth allocated for a class belonging to a policy map.                                                                                                         |
| <b>match discard-class</b>                          | Matches packets of a certain discard-class.                                                                                                                                                  |
| <b>random-detect discard-class-based</b>            | Bases WRED on the discard class value of a packet.                                                                                                                                           |
| <b>random-detect exponential-weighting-constant</b> | Configures the WRED and DWRED exponential weight factor for the average queue size calculation.                                                                                              |
| <b>random-detect precedence</b>                     | Configures WRED and DWRED parameters for a particular IP precedence.                                                                                                                         |
| <b>show policy-map interface</b>                    | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# random-detect discard-class-based

To base weighted random early detection (WRED) on the discard class value of a packet, use the **random-detect discard-class-based** command in policy-map class configuration mode. To disable this feature, use the **no** form of this command.

**random-detect discard-class-based**

**no random-detect discard-class-based**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The defaults are router-dependent.

**Command Modes** Policy-map class configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(13)T   | This command was introduced.                                    |
| 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.  |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** Enter this command so that WRED is based on the discard class instead of on the IP precedence field.

## Examples

The following example shows that random detect is based on the discard class value of a packet:

```
policy-map name
  class-name
    bandwidth percent 40
    random-detect discard-class-based
```

## Related Commands

| Command                    | Description                                 |
|----------------------------|---------------------------------------------|
| <b>match discard-class</b> | Matches packets of a certain discard class. |



# random-detect dscp

To change the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value, use the **random-detect dscp** command in interface or QoS policy-map class configuration mode. To return the minimum and maximum packet thresholds to the default for the DSCP value, use the **no** form of this command.

**random-detect dscp** *dscp-value min-threshold max-threshold [max-probability-denominator]*

**no random-detect dscp** *dscp-value min-threshold max-threshold [max-probability-denominator]*

| Syntax Description                 |  |                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>dscp-value</i>                  |  | DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: <b>af11</b> , <b>af12</b> , <b>af13</b> , <b>af21</b> , <b>af22</b> , <b>af23</b> , <b>af31</b> , <b>af32</b> , <b>af33</b> , <b>af41</b> , <b>af42</b> , <b>af43</b> , <b>cs1</b> , <b>cs2</b> , <b>cs3</b> , <b>cs4</b> , <b>cs5</b> , <b>cs7</b> , <b>ef</b> , or <b>rsvp</b> . |
| <i>min-threshold</i>               |  | Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, Weighted Random Early Detection (WRED) or distributed WRED (dWRED) randomly drops some packets with the specified DSCP value.                                                                                                  |
| <i>max-threshold</i>               |  | Maximum threshold in number of packets. The value range of this argument is from the value of the <i>min-threshold</i> argument to 4096. When the average queue length exceeds the maximum threshold, WRED or dWRED drops all packets with the specified DSCP value.                                                                                                                    |
| <i>max-probability-denominator</i> |  | (Optional) Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is from 1 to 65536. The default is 10; 1 out of every 10 packets is dropped at the maximum threshold.            |

**Command Default** For more information about **random-detect dscp** defaults, see the “Usage Guidelines” section.

**Command Modes** Interface configuration  
Policy-map class configuration

| Command History | Release   | Modification                                                                                                                                                                                                                                   |
|-----------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.1(5)T  | This command was introduced.                                                                                                                                                                                                                   |
|                 | 12.1(5a)E | This command was integrated into Cisco IOS Release 12.1(5a)E in policy-map class configuration mode only.<br><br>The command was introduced for VIP-enabled Cisco 7500 series routers and Catalyst 6000 family switches with a FlexWAN module. |
|                 | 12.0(15)S | This command was integrated into Cisco IOS Release 12.0(15)S in policy-map class configuration mode only.                                                                                                                                      |

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(14)S   | This command was integrated into Cisco IOS Release 12.2(14)S.                                                                                                                     |
| 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                                                                    |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

### Usage Guidelines

Use the **random-detect dscp** command in conjunction with the **random-detect** command in interface configuration mode.

Additionally, the **random-detect dscp** command is available only if you specified the *dscp-based* argument when using the **random-detect** command in interface configuration mode.



#### Note

The **random-detect dscp** command is not available at the interface level for Cisco IOS Release 12.1E or Release 12.0S. The **random-detect dscp** command is available only in policy-map class configuration mode in Cisco IOS Release 12.1E.

### Specifying the DSCP Value

The **random-detect dscp** command allows you to specify the DSCP value per traffic class. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs7**, **ef**, or **rsvp**.

On a particular traffic class, eight DSCP values can be configured per traffic class. Overall, 29 values can be configured on a traffic class: 8 precedence values, 12 AF code points, 1 EF code point, and 8 user-defined DSCP values.

### Assured Forwarding Code Points

The AF code points provide a means for a domain to offer four different levels (four different AF classes). Forwarding assurances for IP packets received from other (such as customer) domains. Each one of the four AF classes is allocated a certain amount of forwarding services (buffer space and bandwidth).

Within each AF class, IP packets are marked with one of three possible drop precedence values (binary 2{010}, 4{100}, or 6{110}), which exist as the three lowest bits in the DSCP header. In congested network environments, the drop precedence value of the packet determines the importance of the packet within the AF class. Packets with higher drop precedence values are discarded before packets with lower drop precedence values.

The upper three bits of the DSCP value determine the AF class; the lower three values determine the drop probability.

### Expedited Forwarding Code Points

The EF code point is usually used to mark high-priority, time-sensitive data. The EF code point marking is equal to the highest precedence value; therefore, the EF code point is always equal to precedence value 7.

### Class Selector Values

The Class Selector (CS) values are equal to IP precedence values (for instance, cs1 is the same as IP precedence 1).

### Default Values

[Table 8](#) lists the default WRED minimum threshold value for each IP precedence value on the distributed platforms.

**Table 8** *Default WRED Minimum Threshold Values for the Distributed Platforms*

| IP (Precedence) | Class Selector (CS) Value | Minimum Threshold Value (Fraction of Maximum Threshold Value) | Important Notes About the Value                                                                        |
|-----------------|---------------------------|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| 0               | cs0                       | 8/16                                                          | All DSCP values that are not configured by the user have the same threshold values as IP precedence 0. |
| 1               | cs1                       | 9/16                                                          | —                                                                                                      |
| 2               | cs2                       | 10/16                                                         | —                                                                                                      |
| 3               | cs3                       | 11/16                                                         | —                                                                                                      |
| 4               | cs4                       | 12/16                                                         | —                                                                                                      |
| 5               | cs5                       | 13/16                                                         | —                                                                                                      |
| 6               | cs6                       | 14/16                                                         | —                                                                                                      |
| 7               | cs7                       | 15/16                                                         | The EF code point is always equal to IP precedence 7.                                                  |

If WRED is using the DSCP value to calculate the drop probability of a packet, all 64 entries of the DSCP table are initialized with the default settings shown in [Table 9](#).

**Table 9** *random-detect dscp Default Settings*

| DSCP (Precedence) | Minimum Threshold | Maximum Threshold | Mark Probability |
|-------------------|-------------------|-------------------|------------------|
| 0(0)              | 20                | 40                | 1/10             |
| 1                 | 22                | 40                | 1/10             |
| 2                 | 24                | 40                | 1/10             |
| 3                 | 26                | 40                | 1/10             |
| 4                 | 28                | 40                | 1/10             |
| 5                 | 30                | 40                | 1/10             |
| 6                 | 32                | 40                | 1/10             |
| 7                 | 34                | 40                | 1/10             |
| 8(1)              | 22                | 40                | 1/10             |
| 9                 | 22                | 40                | 1/10             |
| 10                | 24                | 40                | 1/10             |
| 11                | 26                | 40                | 1/10             |

**Table 9** *random-detect dscp Default Settings (continued)*

| <b>DSCP<br/>(Precedence)</b> | <b>Minimum<br/>Threshold</b> | <b>Maximum<br/>Threshold</b> | <b>Mark<br/>Probability</b> |
|------------------------------|------------------------------|------------------------------|-----------------------------|
| 12                           | 28                           | 40                           | 1/10                        |
| 13                           | 30                           | 40                           | 1/10                        |
| 14                           | 32                           | 40                           | 1/10                        |
| 15                           | 34                           | 40                           | 1/10                        |
| 16(2)                        | 24                           | 40                           | 1/10                        |
| 17                           | 22                           | 40                           | 1/10                        |
| 18                           | 24                           | 40                           | 1/10                        |
| 19                           | 26                           | 40                           | 1/10                        |
| 20                           | 28                           | 40                           | 1/10                        |
| 21                           | 30                           | 40                           | 1/10                        |
| 22                           | 32                           | 40                           | 1/10                        |
| 23                           | 34                           | 40                           | 1/10                        |
| 24(3)                        | 26                           | 40                           | 1/10                        |
| 25                           | 22                           | 40                           | 1/10                        |
| 26                           | 24                           | 40                           | 1/10                        |
| 27                           | 26                           | 40                           | 1/10                        |
| 28                           | 28                           | 40                           | 1/10                        |
| 29                           | 30                           | 40                           | 1/10                        |
| 30                           | 32                           | 40                           | 1/10                        |
| 31                           | 34                           | 40                           | 1/10                        |
| 32(4)                        | 28                           | 40                           | 1/10                        |
| 33                           | 22                           | 40                           | 1/10                        |
| 34                           | 24                           | 40                           | 1/10                        |
| 35                           | 26                           | 40                           | 1/10                        |
| 36                           | 28                           | 40                           | 1/10                        |
| 37                           | 30                           | 40                           | 1/10                        |
| 38                           | 32                           | 40                           | 1/10                        |
| 39                           | 34                           | 40                           | 1/10                        |
| 40(5)                        | 30                           | 40                           | 1/10                        |
| 41                           | 22                           | 40                           | 1/10                        |
| 42                           | 24                           | 40                           | 1/10                        |
| 43                           | 26                           | 40                           | 1/10                        |
| 44                           | 28                           | 40                           | 1/10                        |
| 45                           | 30                           | 40                           | 1/10                        |
| 46                           | 36                           | 40                           | 1/10                        |

**Table 9** *random-detect dscp Default Settings (continued)*

| <b>DSCP<br/>(Precedence)</b> | <b>Minimum<br/>Threshold</b> | <b>Maximum<br/>Threshold</b> | <b>Mark<br/>Probability</b> |
|------------------------------|------------------------------|------------------------------|-----------------------------|
| 47                           | 34                           | 40                           | 1/10                        |
| 48(6)                        | 32                           | 40                           | 1/10                        |
| 49                           | 22                           | 40                           | 1/10                        |
| 50                           | 24                           | 40                           | 1/10                        |
| 51                           | 26                           | 40                           | 1/10                        |
| 52                           | 28                           | 40                           | 1/10                        |
| 53                           | 30                           | 40                           | 1/10                        |
| 54                           | 32                           | 40                           | 1/10                        |
| 55                           | 34                           | 40                           | 1/10                        |
| 56(7)                        | 34                           | 40                           | 1/10                        |
| 57                           | 22                           | 40                           | 1/10                        |
| 58                           | 24                           | 40                           | 1/10                        |
| 59                           | 26                           | 40                           | 1/10                        |
| 60                           | 28                           | 40                           | 1/10                        |
| 61                           | 30                           | 40                           | 1/10                        |
| 62                           | 32                           | 40                           | 1/10                        |
| 63                           | 34                           | 40                           | 1/10                        |
| rsvp                         | 36                           | 40                           | 1/10                        |

**Examples**

The following example enables WRED to use the DSCP value 8. The minimum threshold for the DSCP value 8 is 20, the maximum threshold is 40, and the mark probability is 1/10.

```
random-detect dscp 8 20 40 10
```

**Related Commands**

| <b>Command</b>                 | <b>Description</b>                                      |
|--------------------------------|---------------------------------------------------------|
| <b>random-detect</b>           | Enables WRED or dWRED.                                  |
| <b>show queueing</b>           | Lists all or selected configured queueing strategies.   |
| <b>show queueing interface</b> | Displays the queueing statistics of an interface or VC. |

## random-detect dscp (aggregate)

To configure aggregate Weighted Random Early Detection (WRED) parameters for specific differentiated services code point (DSCP) value, use the **random-detect dscp values (aggregate)** command in QoS policy-map class configuration mode. To disable configuration of aggregate WRED DSCP values, use the **no** form of this command.

**random-detect dscp** *sub-class-val1 sub-class-val2 sub-class-val3 sub-class-val4 min-thresh max-thresh mark-prob*

**no random-detect dscp** *sub-class-val1 sub-class-val2 sub-class-val3 sub-class-val4 min-thresh max-thresh mark-prob*

| Syntax Description    |  |                                                                                                                                                                                                                                                                          |
|-----------------------|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>sub-class-val1</i> |  | DSCP value(s) to which the following WRED profile parameter specifications are to apply. A maximum of eight subclasses (DSCP values) can be specified per command-line interface (CLI) entry. See the “Usage Guidelines” for a list of valid DSCP values.                |
| <i>sub-class-val2</i> |  |                                                                                                                                                                                                                                                                          |
| <i>sub-class-val3</i> |  |                                                                                                                                                                                                                                                                          |
| <i>sub-class-val4</i> |  |                                                                                                                                                                                                                                                                          |
| <i>min-thresh</i>     |  | Minimum number of packets allowed in the queue. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified DSCP value. Valid minimum threshold values are 1 to 16384.                                              |
| <i>max-thresh</i>     |  | Maximum number of packets allowed in the queue. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP value. Valid maximum threshold values are 1 to 16384.                                                        |
| <i>mark-prob</i>      |  | Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. Valid values are 1 to 65535. |

**Command Default** For all precedence levels, the *mark-prob* default value is 10 packets.

**Command Modes** Policy-map class configuration

| Command History | Release     | Modification                                                                                                     |
|-----------------|-------------|------------------------------------------------------------------------------------------------------------------|
|                 | 12.2(18)SXE | This command was introduced.                                                                                     |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                  |
|                 | 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2 and implemented on the Cisco 10000 series router. |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                   |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                  |

**Usage Guidelines**

Use this command with a **random-detect aggregate** command within a policy map configuration. Repeat this command for each set of DSCP values that share WRED parameters.

After the policy map is defined, the policy map must be attached at the virtual circuit (VC) level.

The set of subclass (DSCP precedence) values defined on a **random-detect dscp (aggregate)** CLI are aggregated into a single hardware WRED resource. The statistics for these subclasses are also aggregated.

Use the **show policy-map interface** command to display the statistics for aggregated subclasses.

**DSCP Values**

You must enter one or more differentiated service code point (DSCP) values. The command may include any combination of the following:

- numbers (0 to 63) representing differentiated services code point values
- af numbers (for example, af11) identifying specific AF DSCPs
- cs numbers (for example, cs1) identifying specific CS DSCPs
- **default**—Matches packets with the default DSCP.
- **ef**—Matches packets with EF DSCP.

For example, if you wanted the DSCP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified DSCP values), enter the **match dscp 0 1 2 3 4 5 6 7** command.

**Examples**

The following example shows how to create a class map named map1 and associate it with the policy map named map2. The configuration enables WRED to drop map1 packets based on DSCP 8 with a minimum threshold of 24 and a maximum threshold of 40. The map2 policy map is attached to the outbound gigabitEthernet 0/1 interface.

```
Router(config-if)# class-map map1
Router(config-cmap)# match access-group 10
Router(config-cmap)# exit
Router(config)# policy-map map2
Router(config-pmap)# class map1
Router(config-pmap-c)# bandwidth 48
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp 8 24 40
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy output map2
```

**Related Commands**

| Command                   | Description                                                                                                                                                                   |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>class (policy-map)</b> | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |
| <b>interface</b>          | Configures an interface type and enters interface configuration mode.                                                                                                         |
| <b>policy-map</b>         | Creates a policy map that can be attached to one or more interfaces to specify a service policy.                                                                              |

| Command                          | Description                                                                                                                                                                                          |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>random-detect aggregate</b>   | Enables aggregate WRED and optionally specifies default WRED parameter values for a default aggregate class. This default class is used for all subclasses that have not been explicitly configured. |
| <b>service-policy</b>            | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.                                                          |
| <b>show policy-map interface</b> | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.         |



# random-detect ecn

To enable explicit congestion notification (ECN), use the **random-detect ecn** command in policy-map class configuration mode. To disable ECN, use the **no** form of this command.

**random-detect ecn**

**no random-detect ecn**

**Syntax Description** This command has no arguments or keywords.

**Command Default** By default, ECN is disabled.

**Command Modes** Policy-map class configuration

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(8)T    | This command was introduced.                                    |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** If ECN is enabled, ECN can be used whether Weighted Random Early Detection (WRED) is based on the IP precedence value or the differentiated services code point (DSCP) value.

**Examples** The following example enables ECN in a policy map called “pol1”:

```
Router(config)# policy-map pol1
Router(config-pmap)# class class-default
Router(config-pmap)# bandwidth per 70
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# random-detect ecn
```

| Related Commands | Command                          | Description                                                                                                                                                                         |
|------------------|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>show policy-map</b>           | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.                                                           |
|                  | <b>show policy-map interface</b> | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# random-detect exponential-weighting-constant

To configure the Weighted Random Early Detection (WRED) exponential weight factor for the average queue size calculation for the queue, use the **random-detect exponential-weighting-constant** command in interface configuration mode. To configure the exponential weight factor for the average queue size calculation for the queue reserved for a class, use the **random-detect exponential-weighting-constant** command in policy-map class configuration mode. To return the value to the default, use the **no** form of this command.

**random-detect exponential-weighting-constant** *exponent*

**no random-detect exponential-weighting-constant**

|                           |                                                                                                                                                                                                                                     |                                                                                                                                                                                   |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>exponent</i>                                                                                                                                                                                                                     | Exponent from 1 to 16 used in the average queue size calculation.                                                                                                                 |
| <b>Command Default</b>    | The default exponential weight factor is 9.                                                                                                                                                                                         |                                                                                                                                                                                   |
| <b>Command Modes</b>      | Interface configuration when used on an interface<br><br>Policy-map class configuration when used to specify class policy in a policy map, or when used in the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC). |                                                                                                                                                                                   |
| <b>Command History</b>    | <b>Release</b>                                                                                                                                                                                                                      | <b>Modification</b>                                                                                                                                                               |
|                           | 11.1CC                                                                                                                                                                                                                              | This command was introduced.                                                                                                                                                      |
|                           | 12.0(5)T                                                                                                                                                                                                                            | This command was made available as a QoS policy-map class configuration command.                                                                                                  |
|                           | 12.0(5)XE                                                                                                                                                                                                                           | This command was integrated into Cisco IOS Release 12.0(5)XE and implemented on Versatile Interface Processor (VIP) enabled Cisco 7500 series routers.                            |
|                           | 12.1(5)T                                                                                                                                                                                                                            | This command was integrated into Cisco IOS Release 12.1(5)T and implemented on VIP-enabled Cisco 7500 series routers.                                                             |
|                           | 12.2(33)SRA                                                                                                                                                                                                                         | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                           | 12.2(31)SB                                                                                                                                                                                                                          | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router.                                                                   |
|                           | 12.2SX                                                                                                                                                                                                                              | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                           | 12.4(20)MR                                                                                                                                                                                                                          | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
|                           | 12.2(33)MRA                                                                                                                                                                                                                         | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

---

**Usage Guidelines**

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. Use this command to change the exponent used in the average queue size calculation for WRED services. You can also use this command to configure the exponential weight factor for the average queue size calculation for the queue reserved for a class.

---

**Examples**

The following example configures the policy map called policy1 to contain policy specification for the class called class1. During times of congestion, WRED packet drop is used instead of tail drop. The weight factor used for the average queue size calculation for the queue for class1 is 12.

```
! The following commands create the class map called class1:
class-map class1
  match input-interface FE0/1
```

```
! The following commands define policy1 to contain policy specification for class1:
policy-map policy1
  class class1
    bandwidth 1000
    random-detect
    random-detect exponential-weighting-constant 12
```

The following example configures policy for a traffic class named int10 to configure the exponential weight factor as 12. This is the weight factor used for the average queue size calculation for the queue for traffic class int10. WRED packet drop is used for congestion avoidance for traffic class int10, not tail drop.

```
policy-map policy12
  class int10
    bandwidth 2000
    random-detect exponential-weighting-constant 12
```

| Related Commands | Command                               | Description                                                                                                                                                                                  |
|------------------|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>bandwidth (policy-map class)</b>   | Specifies or modifies the bandwidth allocated for a class belonging to a policy map.                                                                                                         |
|                  | <b>exponential-weighting-constant</b> | Configures the exponential weight factor for the average queue size calculation for a WRED parameter group.                                                                                  |
|                  | <b>fair-queue (class-default)</b>     | Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.                                                                |
|                  | <b>precedence</b>                     | Configures precedence levels for a VC or PVC class that can be assigned to a VC or PVC bundle and thus applied to all of the members of that bundle.                                         |
|                  | <b>precedence (WRED group)</b>        | Configures a WRED group for a particular IP Precedence.                                                                                                                                      |
|                  | <b>random-detect dscp</b>             | Changes the minimum and maximum packet thresholds for the DSCP value.                                                                                                                        |
|                  | <b>random-detect precedence</b>       | Configures WRED and DWRED parameters for a particular IP Precedence.                                                                                                                         |
|                  | <b>show policy-map</b>                | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.                                                                    |
|                  | <b>show policy-map interface</b>      | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |
|                  | <b>show queue</b>                     | Displays the contents of packets inside a queue for a particular interface or VC.                                                                                                            |
|                  | <b>show queueing</b>                  | Lists all or selected configured queueing strategies.                                                                                                                                        |

# random-detect precedence-based

To base weighted random early detection (WRED) on the precedence value of a packet, use the **random-detect precedence-based** command in policy-map class configuration mode. To disable this feature, use the **no** form of this command.

**random-detect precedence-based**

**no random-detect precedence-based**

**Syntax Description** This command has no arguments or keywords.

**Command Default** WRED is disabled by default.

**Command Modes** Policy-map class configuration (config-pmap-c)

| Command History | Release     | Modification                                                                                        |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------|
|                 | 12.0(28)S   | This command was introduced. (as <b>random-detect prec-based</b> )                                  |
|                 | 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.                                      |
|                 | 12.4(20)T   | This command was replaced by the <b>random-detect precedence-based</b> command within a policy map. |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                      |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                     |
|                 |             |                                                                                                     |

**Usage Guidelines** With the **random-detect precedence-based** command, WRED is based on the IP precedence value of the packet.

Use the **random-detect precedence-based** command before configuring the **random-detect precedence** command.

Use the **random-detect precedence** command when you configure a policy map.

**Examples**

The following example shows that random detect is based on the precedence value of a packet:

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 80
Router(config-pmap-c)# random-detect precedence-based
Router(config-pmap-c)# random-detect precedence 2 500 ms 1000 ms
Router(config-pmap-c)# exit
```

**Related Commands**

| Command                         | Description                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>random-detect</b>            | Enables WRED or DWRED.                                                                                                                                                 |
| <b>random-detect precedence</b> | Configures the WRED and DWRED parameters for a particular IP precedence; configures WRED parameters for a particular IP precedence for a class policy in a policy map. |

# recovered-clock recovered

The **recovered-clock recovered** command allows you to configure in-band pseudowire-based active clock recovery on a CEM interface. To disable this feature, use the **no** form of this command.

**recovered-clock recovered adaptive cem** *subslot-number* *port-number* *cem-group-number*

**no recovered-clock recovered adaptive cem** *subslot-number* *port-number* *cem-group-number*

## Syntax Description

|                         |                                                                          |
|-------------------------|--------------------------------------------------------------------------|
| <b>adaptive</b>         | Specifies the clock recovery type.                                       |
| <b>cem</b>              | Specifies the Circuit emulation (CEM) interface for the recovered clock. |
| <i>subslot-number</i>   | Subslot of the CEM interface for the recovered clock.                    |
| <i>port-number</i>      | Port number of the CEM interface for the recovered clock.                |
| <i>cem-group-number</i> | CEM group to which the clock applies.                                    |

## Command Default

There is no default setting.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(19)MR2 | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

For more information about adaptive clock recovery, see the [“Configuring Clocking and Timing” section on page 4-39](#).

## Examples

The following example shows how to use the **recovered-clock recovered** command:

```
Router# config t
Router(config)# recovered-clock recovered adaptive cem 0 0 0
Router(config)# exit
```

## Related Commands

| Command                      | Description                                         |
|------------------------------|-----------------------------------------------------|
| <b>recovered-clock slave</b> | Allows you to configure out-of-band clock recovery. |

# recovered-clock slave

To configure out-of-band clock recovery, use the **recovered-clock slave** command. This command automatically creates a virtual-cem interface. To access the virtual-cem interface, use the command **interface virtual-cem 0/24**. To disable this feature, use the feature, use the **no** form of this command.

**recovered-clock slave**

**no recovered-clock slave**

**Syntax Description** This command has no arguments or keywords.

**Command Default** There is no default setting.

**Command Modes** Global configuration

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(19)MR2 | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Examples** The following example shows how to use the **recovered-clock slave** command and how to configure the virtual-cem interface:

```
Router# config t
Router(config)# recovered-clock slave
Router(config-if)# interface virtual-cem 0/24
Router(config-if)# payload-size 486
Router(config-if)# cem 0
Router(config-if)# xconnect 10.10.10.2 7600 encaps mpls
Router(config-if)# exit
Router(config)# exit
```

| Related Commands | Command                          | Description                         |
|------------------|----------------------------------|-------------------------------------|
|                  | <b>recovered-clock recovered</b> | Configures adaptive clock recovery. |



# rep admin vlan

Use the **rep admin vlan** global configuration command to configure a Resilient Ethernet Protocol (REP) administrative VLAN for REP to transmit hardware flood layer (HFL) messages. Use the **no** form of this command to return to the default configuration with VLAN 1 as the administrative VLAN.

**rep admin vlan** *vlan-id*

**no rep admin vlan**

|                           |                |                                                                                              |
|---------------------------|----------------|----------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>vlan-id</i> | VLAN ID range is from 1 to 4094. The default is VLAN 1; the range to configure is 2 to 4094. |
|---------------------------|----------------|----------------------------------------------------------------------------------------------|

|                        |                                    |
|------------------------|------------------------------------|
| <b>Command Default</b> | The administrative VLAN is VLAN 1. |
|------------------------|------------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

| <b>Command History</b> | Release     | Modification                                                    |
|------------------------|-------------|-----------------------------------------------------------------|
|                        | 12.2(40)SE  | This command was introduced.                                    |
|                        | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | If the VLAN does not already exist, this command does not create the VLAN.                                                                                                                                                                                                                                                                                                                                                                                                  |
|                         | To avoid the delay introduced by relaying messages in software for link-failure or VLAN-blocking notification during load balancing, REP floods packets at the hardware flood layer (HFL) to a regular multicast address. These messages are flooded to the whole network, not just the REP segment. Switches that do not belong to the segment treat them as data traffic. Configuring an administrative VLAN for the whole domain can control flooding of these messages. |
|                         | If no REP administrative VLAN is configured, the default is VLAN 1.                                                                                                                                                                                                                                                                                                                                                                                                         |
|                         | There can be only one administrative VLAN on a switch and on a segment.                                                                                                                                                                                                                                                                                                                                                                                                     |
|                         | The administrative VLAN cannot be the RSPAN VLAN.                                                                                                                                                                                                                                                                                                                                                                                                                           |

|                 |                                                                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | This example shows how to configure VLAN 100 as the REP administrative VLAN:                           |
|                 | Router (config)# <b>rep admin vlan 100</b>                                                             |
|                 | You can verify your settings by entering the <b>show interface rep detail</b> privileged EXEC command. |

| <b>Related Commands</b> | Command                           | Description                                                                                                                      |
|-------------------------|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
|                         | <b>show interfaces rep detail</b> | Displays detailed REP configuration and status for all interfaces or the specified interface, including the administrative VLAN. |

# rep block port

Use the **rep block port** interface configuration command on the REP primary edge port to configure Resilient Ethernet Protocol (REP) VLAN load balancing. Use the **no** form of this command to return to the default configuration.

**rep block port** {*id port-id* | *neighbor\_offset* | **preferred**} **vlan** {*vlan-list* | **all**}

**no rep block port** {*id port-id* | *neighbor\_offset* | **preferred**}

## Syntax Description

|                          |                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>id</b> <i>port-id</i> | Identifies the VLAN blocking alternate port, a unique port ID that is automatically generated when REP is enabled. The REP port ID is a 16-character hexadecimal value. You can view the port ID for an interface by entering the <b>show interface interface-id rep detail</b> command.                                                                               |
| <i>neighbor_offset</i>   | Identifies the VLAN blocking alternate port, the offset number of a neighbor. The range is -256 to +256; a value of 0 is invalid. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors. |
| <b>preferred</b>         | Identifies the VLAN blocking alternate port as the segment port on which you entered the <b>rep segment segment-id preferred</b> interface configuration command.<br><br><b>Note</b> Entering the <b>preferred</b> keyword does not ensure that the preferred port is the alternate port; it gives it preference over other similar ports.                             |
| <b>vlan</b>              | Identify the VLANs to be blocked.                                                                                                                                                                                                                                                                                                                                      |
| <i>vlan-list</i>         | Enter a VLAN ID from 1 to 4094 or a range or sequence of VLANs (such as 1-3, 22, 41-44) of VLANs to be blocked.                                                                                                                                                                                                                                                        |
| <b>all</b>               | Blocks all VLANs.                                                                                                                                                                                                                                                                                                                                                      |

## Command Default

The default behavior after you enter the **rep preempt segment** privileged EXEC command (for manual preemption) is to block all VLANs at the primary edge port. This behavior remains until you configure the **rep block port** command.

If the primary edge port cannot determine which port is to be the alternate port, the default action is no preemption and no VLAN load balancing.

## Command Modes

Interface configuration

## Command History

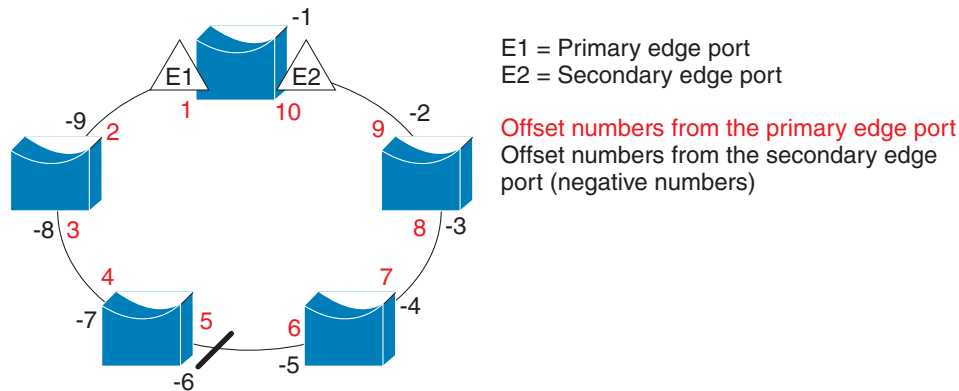
| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(40)SE  | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines**

You must enter this command on the REP primary edge port.

When you select an alternate port by entering an offset number, this number identifies the downstream neighbor port of an edge port. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors. [Figure B-2](#) shows a REP segment with a blocked port.

**Figure B-2 Neighbor Offset Numbers in a REP Segment**



201890

**Note**

You would never enter an offset value of 1 because that is the offset number of the primary edge port itself.

If you have configured a preempt delay time by entering the **rep preempt delay seconds** interface configuration command and a link failure and recovery occurs, VLAN load balancing begins after the configured preemption time period elapses without another link failure. The alternate port specified in the load-balancing configuration blocks the configured VLANs and unblocks all other segment ports. If the primary edge port cannot determine the alternate port for VLAN balancing, the default action is no preemption.

Each port in a segment has a unique port ID. The port ID format is similar to the one used by the spanning tree algorithm: a port number (unique on the bridge) associated to a MAC address (unique in the network). To determine the port ID of a port, enter the **show interface interface-id rep detail** command.

**Examples**

This example shows how to configure REP VLAN load balancing on the Switch B primary edge port (Gigabit Ethernet port 0/1) and to configure Gigabit Ethernet port 0/2 of Switch A as the alternate port to block VLANs 1 to 100. The alternate port is identified by its port ID, shown in bold in the output of the **show interface rep detail** command for the Switch A port.

```
Switch A# show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB17800EEE
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 1
Preempt Delay Timer: 35 sec
```

```

Load-balancing block port: none
Load-balancing block vlan: none
STCN Propagate to:
PDU/TLV statistics:
LSL PDU rx: 107122, tx: 192493

```

```

Router# config t
Router (config)# interface gigabitethernet0/1
Router (config-if)# rep block port id 0080001647FB1780 vlan 1-100
Router (config-if)# exit

```

This example shows how to configure VLAN load balancing by using a neighbor offset number and how to verify the configuration by entering the **show interfaces rep detail** privileged EXEC command:

```

Router# config t
Router (config)# interface gigabitethernet0/2
Router (config-if)# rep block port 6 vlan 1-110
Router (config-if)# end

Router# show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB178009C3
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 3
Preempt Delay Timer: 35 sec
Load-balancing block port: 6
Load-balancing block vlan: 1-110
STCN Propagate to: none
LSL PDU rx: 1466780, tx: 3056637
HFL PDU rx: 2, tx: 0
BPA TLV rx: 1, tx: 2119695
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 757406, tx: 757400
EPA-COMMAND TLV rx: 1, tx: 1
EPA-INFO TLV rx: 178326, tx: 178323

```

## Related Commands

| Command                           | Description                                                                                                                      |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>rep preempt delay</b>          | Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.               |
| <b>rep preempt segment</b>        | Manually starts REP VLAN load balancing on a segment.                                                                            |
| <b>show interfaces rep detail</b> | Displays REP detailed configuration and status for all interfaces or the specified interface, including the administrative VLAN. |

# rep preempt delay

Use the **rep preempt delay** interface configuration command on the REP primary edge port to configure a waiting period after a segment port failure and recovery before Resilient Ethernet Protocol (REP) VLAN load balancing is triggered. Use the **no** form of this command to remove the configured delay.

**rep preempt delay** *seconds*

**no rep preempt delay**

|                           |                                                                                   |
|---------------------------|-----------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>seconds</i> Number of seconds to delay REP preemption. The range is 15 to 300. |
|---------------------------|-----------------------------------------------------------------------------------|

|                        |                                                                                                                                       |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>Command Default</b> | No preemption delay is set. If you do not enter the <b>rep preempt delay</b> command, the default is manual preemption with no delay. |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | Interface configuration |
|----------------------|-------------------------|

|                        |                |                                                                 |
|------------------------|----------------|-----------------------------------------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                             |
|                        | 12.2(40)SE     | This command was introduced.                                    |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | You must enter this command on the REP primary edge port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                         | You must enter this command and configure a preempt time delay if you want VLAN load balancing to automatically trigger after a link failure and recovery.                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                         | If VLAN load balancing is configured, after a segment port failure and recovery, the REP primary edge port starts a delay timer before VLAN load balancing occurs. Note that the timer restarts after each link failure. When the timer expires, the REP primary edge alerts the alternate port to perform VLAN load balancing (configured by using the <b>rep block port</b> interface configuration command) and prepares the segment for the new topology. The configured VLAN list is blocked at the alternate port, and all other VLANs are blocked at the primary edge port. |

|                 |                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | This example shows how to configure a REP preemption time delay of 100 seconds on the primary edge port:                                         |
|                 | <pre>Router (config)# <b>interface gigabitethernet0/1</b> Router (config-if)# <b>rep preempt delay 100</b> Router (config-if)# <b>exit</b></pre> |
|                 | You can verify your settings by entering the <b>show interfaces rep</b> privileged EXEC command.                                                 |

■ rep preempt delay

| Related Commands | Command             | Description                                                                        |
|------------------|---------------------|------------------------------------------------------------------------------------|
|                  | rep block port      | Configures VLAN load balancing.                                                    |
|                  | show interfaces rep | Displays REP configuration and status for all interfaces or a specified interface. |

# rep preempt segment

Use the **rep preempt segment** privileged EXEC command to manually start Resilient Ethernet Protocol (REP) VLAN load balancing on a segment.

**rep preempt segment** *segment\_id*

|                           |                                                                       |
|---------------------------|-----------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>segment-id</i> ID of the REP segment. The range is from 1 to 1024. |
|---------------------------|-----------------------------------------------------------------------|

|                        |                                            |
|------------------------|--------------------------------------------|
| <b>Command Default</b> | Manual preemption is the default behavior. |
|------------------------|--------------------------------------------|

|                      |                 |
|----------------------|-----------------|
| <b>Command Modes</b> | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(40)SE  | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                                                                                                                                                                                                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | When you enter the <b>rep preempt segment</b> <i>segment-id</i> command, a confirmation message appears before the command is executed because preemption can cause network disruption.                                                                                                    |
|                         | Enter this command on the switch on the segment that has the primary edge port.                                                                                                                                                                                                            |
|                         | If you do not configure VLAN load balancing, entering this command results in the default behavior—the primary edge port blocks all VLANs.                                                                                                                                                 |
|                         | You configure VLAN load balancing by entering the <b>rep block port</b> { <i>id port-id</i>   <i>neighbor_offset</i>   <b>preferred</b> } <b>vlan</b> { <i>vlan-list</i>   <b>all</b> } interface configuration command on the REP primary edge port before you manually start preemption. |
|                         | There is not a <b>no</b> version of this command.                                                                                                                                                                                                                                          |

|                 |                                                                                                         |
|-----------------|---------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | This example shows how to manually trigger REP preemption on segment 100 with the confirmation message: |
|                 | Router# <b>rep preempt segment 100</b>                                                                  |
|                 | The command will cause a momentary traffic disruption.                                                  |
|                 | Do you still want to continue? [confirm]                                                                |

| Related Commands | Command                                      | Description                                                                          |
|------------------|----------------------------------------------|--------------------------------------------------------------------------------------|
|                  | <b>rep block port</b>                        | Configures VLAN load balancing.                                                      |
|                  | <b>show interfaces rep</b> [ <b>detail</b> ] | Displays REP configuration and status for all interfaces or the specified interface. |

## rep segment

Use the **rep segment** interface configuration command to enable Resilient Ethernet Protocol (REP) on the interface and to assign a segment ID to it. Use the **no** form of this command to disable REP on the interface.

**rep segment** *segment-id* [**edge** [**primary**]] [**preferred**]

**no rep segment**

### Syntax Description

|                   |                                                                                                                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>segment-id</i> | Assigns a segment ID to the interface. The range is from 1 to 1024.                                                                                                                                                                                                                                                                          |
| <b>edge</b>       | (Optional) Identifies the interface as one of the two REP edge ports. Entering the <b>edge</b> keyword without the <b>primary</b> keyword configures the port as the secondary edge port.                                                                                                                                                    |
| <b>primary</b>    | (Optional) On an edge port, specifies that the port is the primary edge port. A segment has only one primary edge port. If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one of them to serve as the segment primary edge port.                                    |
| <b>preferred</b>  | (Optional) Specifies that the port is the preferred alternate port or the preferred port for VLAN load balancing.<br><br><b>Note</b> Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port. |

### Command Default

REP is disabled on the interface.

When REP is enabled on an interface, the default is for the port to be a regular segment port.

### Command Modes

Interface configuration

### Command History

| Release     | Modification                                                                                                                         |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(40)SE  | This command was introduced.                                                                                                         |
| 12.2(50)SE  | The <b>no-neighbor</b> keyword was added.                                                                                            |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. Release 12.2(33)MRA does not support the <b>no-neighbor</b> keyword. |

### Usage Guidelines

REP ports must be Layer 2 trunk ports.

REP ports should not be configured as one of these port types:

- SPAN destination port
- Private VLAN port
- Tunnel port



- Access port
- REP ports must be network node interfaces (NNIs). REP ports cannot be user-network interfaces (UNIs) or enhanced network interfaces (ENIs).

You must configure two edge ports on each REP segment, a primary edge port and a port to act as a secondary edge port. If you configure two ports in a segment as the primary edge port, for example ports on different switches, the configuration is allowed, but the REP selects one of them to serve as the segment primary edge port.

REP ports follow these rules:

- There is no limit to the number of REP ports on a switch; however, only two ports on a switch can belong to the same REP segment.
- If only one port on a switch is configured in a segment, the port should be an edge port.
- If two ports on a switch belong to the same segment, they must be both edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and regular segment port on a switch cannot belong to the same segment.
- Release 12.2(33)MRA does not support the **no-neighbor** keyword.
- If two ports on a switch belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.

If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one of them to serve as the segment primary edge port. Enter the **show rep topology** privileged EXEC command on a port in the segment to verify which port is the segment primary edge port.

REP interfaces come up in a blocked state and remain in a blocked state until notified that it is safe to unblock. You need to be aware of this to avoid sudden connection losses.

You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

---

## Examples

This example shows how to enable REP on a regular (nonedge) segment port:

```
Router (config)# interface gigabitethernet0/1
Router (config-if)# rep segment 100
```

This example shows how to enable REP on a port and to identify the port as the REP primary edge port:

```
Router (config)# interface gigabitethernet0/2
Router (config-if)# rep segment 100 edge primary
```

This example shows how to enable REP on a port and to identify the port as the REP secondary edge port:

```
Router (config)# interface gigabitethernet0/2
Router (config-if)# rep segment 100 edge
```

You can verify your settings by entering the **show interfaces rep** privileged EXEC command. To verify which port in the segment is the primary edge port, enter the **show rep topology** privileged EXEC command.

| Related Commands | Command                             | Description                                                                                                                    |
|------------------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>show interfaces rep [detail]</b> | Displays REP configuration and status for all interfaces or the specified interface.                                           |
|                  | <b>show rep topology [detail]</b>   | Displays information about all ports in the segment, including which one was configured and selected as the primary edge port. |

# rep stcn

Use the **rep stcn** interface configuration command on a Resilient Ethernet Protocol (REP) edge port to configure the port to send REP segment topology change notifications (STCNs) to another interface, to other segments, or to Spanning Tree Protocol (STP) networks. Use the **no** form of this command to disable the sending of STCNs to the interface, segment, or STP network.

**rep stcn** {**interface** *interface-id* | **segment** *id-list* | **stp**}

**no rep stcn** {**interface** | **segment** | **stp**}

## Syntax Description

|                                      |                                                                                                                                                                    |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>interface</b> <i>interface-id</i> | Identifies a physical interface or port channel to receive STCNs.                                                                                                  |
| <b>segment</b> <i>id-list</i>        | Identifies one REP segment or list of segments to receive STCNs. The range is 1 to 1024. You can also configure a sequence of segments (for example 3-5, 77, 100). |
| <b>stp</b>                           | Specifies that the router send STCNs to an STP network.                                                                                                            |

## Command Default

Transmission of STCNs to other interfaces, segments, or STP networks is disabled.

## Command Modes

Interface configuration

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(40)SE  | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

Enter this command on a segment edge port.

You use this command to notify other portions of the Layer 2 network of topology changes that occur in the local REP segment. This removes obsolete entries in the Layer 2 forwarding table in other parts of the network, which allows faster network convergence.

## Examples

This example shows how to configure the REP primary edge port to send STCNs to segments 25 to 50:

```
Router (config)# interface gigabitethernet0/2
Router (config-if)# rep stcn segment 25-50
Router (config-if)# exit
```

You can verify your settings by entering the **show interfaces rep detail** privileged EXEC command.

## Related Commands

| Command                             | Description                                                                          |
|-------------------------------------|--------------------------------------------------------------------------------------|
| <b>show interfaces rep [detail]</b> | Displays REP configuration and status for all interfaces or the specified interface. |

# router bgp

To configure the BGP routing process, use the **router bgp** command in global configuration mode. To remove a routing process, use the **no** form of this command.

**router bgp** *autonomous-system-number*

**no router bgp** *autonomous-system-number*

## Syntax Description

|                                 |                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>autonomous-system-number</i> | Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. Valid values are 1 to 65535.<br><br>For more details about autonomous system number formats, see the Usage Guidelines section. |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Command Default

No BGP routing process is configured by default.

## Command Modes

Global configuration (config)

## Command History

| Release                  | Modification                                                                                                                                  |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 10.0                     | This command was introduced.                                                                                                                  |
| 12.2(25)SG               | This command was integrated into Cisco IOS Release 12.2(25)SG.                                                                                |
| 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                               |
| 12.2(31)SB2              | This command was integrated into Cisco IOS Release 12.2(31)SB2.                                                                               |
| 12.2(33)SRB              | This command was modified. Support for IPv6 was added.                                                                                        |
| 12.2(14)SX               | This command was integrated into Cisco IOS Release 12.2(14)SX.                                                                                |
| 12.2(33)SB               | This command was modified. Support for IPv6 was added.                                                                                        |
| 12.0(32)S12              | This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.                                     |
| 12.0(32)SY8              | This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.                              |
| 12.4(24)T                | This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.                                     |
| Cisco IOS XE Release 2.3 | This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.                                     |
| 12.2(33)SX11             | This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.                              |
| 12.0(33)S3               | This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain. |
| Cisco IOS XE Release 2.4 | This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain. |

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

### Usage Guidelines

This command allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Prior to January 2009, BGP autonomous system numbers that were allocated to companies were 2-octet numbers in the range from 1 to 65535 as described in RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*. Due to increased demand for autonomous system numbers, the Internet Assigned Number Authority (IANA) starts in January 2009 to allocate four-octet autonomous system numbers in the range from 65536 to 4294967295. RFC 5396, *Textual Representation of Autonomous System (AS) Numbers*, documents three methods of representing autonomous system numbers. Cisco has implemented the following two methods:

- **Asplain**—Decimal value notation where both 2-byte and 4-byte autonomous system numbers are represented by their decimal value. For example, 65526 is a 2-byte autonomous system number and 234567 is a 4-byte autonomous system number.
- **Asdot**—Autonomous system dot notation where 2-byte autonomous system numbers are represented by their decimal value and 4-byte autonomous system numbers are represented by a dot notation. For example, 65526 is a 2-byte autonomous system number and 1.169031 is a 4-byte autonomous system number (this is dot notation for the 234567 decimal number).

For details about the third method of representing autonomous system numbers, see RFC 5396.

#### Asdot Only Autonomous System Number Formatting

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, the 4-octet (4-byte) autonomous system numbers are entered and displayed only in asdot notation, for example, 1.10 or 45000.64000. When using regular expressions to match 4-byte autonomous system numbers the asdot format includes a period which is a special character in regular expressions. A backslash must be entered before the period for example, 1\.14, to ensure the regular expression match does not fail. [Table 10](#) shows the format in which 2-byte and 4-byte autonomous system numbers are configured, matched in regular expressions, and displayed in **show** command output in Cisco IOS images where only asdot formatting is available.

**Table 10 Asdot Only 4-Byte Autonomous System Number Format**

| Format | Configuration Format                             | Show Command Output and Regular Expression Match Format |
|--------|--------------------------------------------------|---------------------------------------------------------|
| asdot  | 2-byte: 1 to 65535<br>4-byte: 1.0 to 65535.65535 | 2-byte: 1 to 65535<br>4-byte: 1.0 to 65535.65535        |

#### Asplain as Default Autonomous System Number Formatting

In Cisco IOS Release 12.0(32)SY8, 12.2(33)SX11, 12.0(33)S3, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain as the default display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain and asdot format. In addition, the default format for matching 4-byte autonomous system numbers in regular expressions is asplain, so you must ensure that any regular expressions to match 4-byte autonomous system numbers are written in the asplain format. If you want to change the default **show** command output to display 4-byte autonomous system numbers in the asdot

format, use the **bgp asnotation dot** command under router configuration mode. When the asdot format is enabled as the default, any regular expressions to match 4-byte autonomous system numbers must be written using the asdot format, or the regular expression match fails. Table 11 and Table 12 show that although you can configure 4-byte autonomous system numbers in either asplain or asdot format, only one format is used to display **show** command output and control 4-byte autonomous system number matching for regular expressions, and the default is asplain format. To display 4-byte autonomous system numbers in **show** command output and to control matching for regular expressions in the asdot format, you must configure the **bgp asnotation dot** command. After enabling the **bgp asnotation dot** command, a hard reset must be initiated for all BGP sessions by entering the **clear ip bgp \*** command.

**Note**

If you are upgrading to an image that supports 4-byte autonomous system numbers, you can still use 2-byte autonomous system numbers. The **show** command output and regular expression match are not changed and remain in asplain (decimal value) format for 2-byte autonomous system numbers regardless of the format configured for 4-byte autonomous system numbers.

**Table 11** Default Asplain 4-Byte Autonomous System Number Format

| Format  | Configuration Format                              | Show Command Output and Regular Expression Match Format |
|---------|---------------------------------------------------|---------------------------------------------------------|
| asplain | 2-byte: 1 to 65535<br>4-byte: 65536 to 4294967295 | 2-byte: 1 to 65535<br>4-byte: 65536 to 4294967295       |
| asdot   | 2-byte: 1 to 65535<br>4-byte: 1.0 to 65535.65535  | 2-byte: 1 to 65535<br>4-byte: 65536 to 4294967295       |

**Table 12** Asdot 4-Byte Autonomous System Number Format

| Format  | Configuration Format                              | Show Command Output and Regular Expression Match Format |
|---------|---------------------------------------------------|---------------------------------------------------------|
| asplain | 2-byte: 1 to 65535<br>4-byte: 65536 to 4294967295 | 2-byte: 1 to 65535<br>4-byte: 1.0 to 65535.65535        |
| asdot   | 2-byte: 1 to 65535<br>4-byte: 1.0 to 65535.65535  | 2-byte: 1 to 65535<br>4-byte: 1.0 to 65535.65535        |

### Reserved and Private Autonomous System Numbers

In Cisco IOS Release 12.0(32)S12, 12.0(32)SY8, 12.2(33)SX11, 12.4(24)T, Cisco IOS XE Release 2.3 and later releases, the Cisco implementation of BGP supports RFC 4893. RFC 4893 was developed to allow BGP to support a gradual transition from 2-byte autonomous system numbers to 4-byte autonomous system numbers.

**Note**

A new reserved (private) autonomous system number, 23456, was created by RFC 4893 and this number cannot be configured as an autonomous system number in the Cisco IOS CLI.

RFC 5398, *Autonomous System (AS) Number Reservation for Documentation Use*, describes new reserved autonomous system numbers for documentation purposes. Use of the reserved numbers allow configuration examples to be accurately documented and avoids conflict with production networks if these configurations are literally copied. The reserved numbers are documented in the IANA

autonomous system number registry. Reserved 2-byte autonomous system numbers are in the contiguous block, 64496 to 64511 and reserved 4-byte autonomous system numbers are from 65536 to 65551 inclusive.

Private 2-byte autonomous system numbers are still valid in the range from 64512 to 65534 with 65535 being reserved for special use. Private autonomous system numbers can be used for internal routing domains but must be translated for traffic that is routed out to the Internet. BGP should not be configured to advertise private autonomous system numbers to external networks. Cisco IOS software does not remove private autonomous system numbers from routing updates by default. We recommend that ISPs filter private autonomous system numbers.

**Note**

Autonomous system number assignment for public and private networks is governed by the IANA. For information about autonomous-system numbers, including reserved number assignment, or to apply to register an autonomous system number, see the following URL: <http://www.iana.org/>.

**Examples**

The following example configures a BGP process for autonomous system 45000 and configures two external BGP neighbors in different autonomous systems using 2-byte autonomous system numbers:

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
 exit-address-family
```

The following example configures a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain notation. This example is supported in Cisco IOS Release 12.0(32)SY8, 12.2(33)SX11, 12.0(33)S3, Cisco IOS XE Release 2.4, and later releases.

```
router bgp 65538
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
 exit-address-family
```

The following example configures a BGP process for autonomous system 1.2 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asdot notation.

```
router bgp 1.2
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
```

## router bgp

```
address-family ipv4
neighbor 192.168.1.2 activate
neighbor 192.168.3.2 activate
no auto-summary
```

**Related Commands**

| Command                                    | Description                                                                                                                                                |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bgp asnotation dot</b>                  | Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation. |
| <b>neighbor remote-as</b>                  | Adds an entry to the BGP or multiprotocol BGP neighbor table.                                                                                              |
| <b>network (BGP and multiprotocol BGP)</b> | Specifies the list of networks for the BGP routing process.                                                                                                |



# router isis

To enable the Intermediate System-to-Intermediate System (IS-IS) routing protocol and to specify an IS-IS process, use the **router isis** command in global configuration mode. To disable IS-IS routing, use the **no** form of this command.

**router isis** *area-tag*

**no router isis** *area-tag*

## Syntax Description

|                 |                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>area-tag</i> | Meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router.<br><br>Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration. |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Command Default

This command is disabled by default.

## Command Modes

Global configuration

## Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.0        | This command was introduced.                                                                                                                                                      |
| 12.0(5)T    | Multiarea functionality was added, changing the way the <i>tag</i> argument (now <i>area-tag</i> ) is used.                                                                       |
| 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                                                                    |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

## Usage Guidelines

This command is used to enable routing for an area. An appropriate network entity title (NET) must be configured to specify the area address of the area and system ID of the router. Routing must be enabled on one or more interfaces before adjacencies may be established and dynamic routing is possible.

If you have IS-IS running and at least one International Standards Organization Interior Gateway Routing Protocol (ISO-IGRP) process, the IS-IS process and the ISO-IGRP process cannot both be configured without an area tag. The null tag can be used by only one process. If you run ISO-IGRP and IS-IS, a null tag can be used for IS-IS, but not for ISO-IGRP at the same time. However, each area in an IS-IS multiarea configuration should have a nonnull area tag to facilitate identification of the area.

You can configure only one IS-IS routing process to perform Level 2 (interarea) routing. You can configure this process to perform Level 1 (intra-area) routing at the same time. You can configure up to 29 additional processes as Level 1-only processes. If Level 2 routing is configured on any process, all additional processes are automatically configured as Level 1.

An interface cannot be part of more than one area, except in the case where the associated routing process is performing both Level 1 and Level 2 routing. On media such as WAN media where subinterfaces are supported, different subinterfaces could be configured for different areas.

If Level 2 routing is not desired for a given area, use the **is-type** command to remove Level 2. Level 2 routing can then be enabled on some other router instance.

Explicit redistribution between IS-IS instances is prohibited (prevented by the parser). In other words, you cannot issue a **redistribute isis area-tag** command in the context of another IS-IS router instance (**router isis area-tag**). Redistribution from any other routing protocol into a particular area is possible, and is configured per router instance, as in Cisco IOS software Release 12.0, using the **redistribute** and **route map** commands. By default, redistribution is into Level 2.

If multiple Level 1 areas are defined, the Target Address Resolution Protocol (TARP) behaves in the following way:

- The locally assigned target identifier gets the network service access point (NSAP) of the Level 2 area, if present.
- If only Level 1 areas are configured, the router uses the NSAP of the first active Level 1 area as shown in the configuration at the time of TARP configuration (“tarp run”). (Level 1 areas are sorted alphanumerically by tag name, with capital letters coming before lowercase letters. For example, AREA-1 precedes AREA-2, which precedes area-1.) Note that the target identifier NSAP could change following a reload if a new Level 1 area is added to the configuration after TARP is running.
- The router continues to process all Type 1 and 2 protocol data units (PDUs) that are for this router. Type 1 PDUs are processed locally if the specified target identifier is in the local target identifier cache. If not, they are “propagated” (routed) to all interfaces in the *same* Level 1 area. (The same area is defined as the area configured on the input interface.)
- Type 2 PDUs are processed locally if the specified target identifier is in the local target identifier cache. If not, they are propagated via all interfaces (all Level 1 or Level 2 areas) with TARP enabled. If the source of the PDU is from a different area, the information is also added to the local target identifier cache. Type 2 PDUs are propagated via all static adjacencies.
- Type 4 PDUs (for changes originated locally) are propagated to all Level 1 and Level 2 areas (because internally they are treated as “Level 1-2”).
- Type 3 and 5 PDUs continue to be routed.
- Type 1 PDUs are propagated only via Level 1 static adjacencies if the static NSAP is in one of the Level 1 areas in this router.

After you enter the **router isis** command, you can enter the maximum number of paths. There can be from 1 to 32 paths.

## Examples

The following example configures IS-IS for IP routing, with system ID 0000.0000.0002 and area ID 01.0001, and enables IS-IS to form adjacencies on Ethernet interface 0 and serial interface 0. The IP prefix assigned to Ethernet interface 0 is advertised to other IS-IS routers.

```
router isis tag1
 net 01.0001.0000.0000.0002
 is-type level-1
!
```

```
interface ethernet 0
 ip address 10.1.1.1 255.255.255.0
 ip router isis
!
```

```
interface serial 0
 ip unnumbered ethernet0
 ip router isis
```

The following example starts IS-IS routing with the optional *area-tag* argument, where CISCO is the value for the *area-tag* argument:

```
router isis CISCO
```

The following example specifies IS-IS as an IP routing protocol for a process named Finance, and specifies that the Finance process is routed on Ethernet interface 0 and serial interface 0:

```
router isis Finance
 net 49.0001.aaaa.aaaa.aaaa.00
interface Ethernet 0
 ip router isis Finance
interface serial 0
 ip router isis Finance
```

The following example shows usage of the **maximum-paths** option:

```
router isis
maximum-paths?
20
```

#### Related Commands

| Command                  | Description                                                                                                        |
|--------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>clns router isis</b>  | Enables IS-IS routing for ISO CLNS on an interface and attaches an area designator to the routing process.         |
| <b>ip router isis</b>    | Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process. |
| <b>net</b>               | Configures an IS-IS NET for the routing process.                                                                   |
| <b>redistribute (IP)</b> | Redistribute routes from one routing domain into another routing domain.                                           |
| <b>route-map (IP)</b>    | Defines the conditions for redistributing routes from one routing protocol into another.                           |

# router ospf

To configure an Open Shortest Path First (OSPF) routing process, use the **router ospf** command in global configuration mode. To terminate an OSPF routing process, use the **no** form of this command.

**router ospf** *process-id* [**vrf** *vpn-name*]

**no router ospf** *process-id* [**vrf** *vpn-name*]

|                           |                            |                                                                                                                                                                                         |
|---------------------------|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>process-id</i>          | Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process. |
|                           | <b>vrf</b> <i>vpn-name</i> | (Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with OSPF VRF processes.                                                                    |

**Command Default** No OSPF routing process is defined.

**Command Modes** Global configuration

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                                                               |
|------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | 10.0           | This command was introduced.                                                                                                                                                      |
|                        | 12.0(7)T       | The <b>vrf</b> keyword and <i>vpn-name</i> arguments were added to identify a VPN.                                                                                                |
|                        | 12.0(9)ST      | The <b>vrf</b> keyword and <i>vpn-name</i> arguments were added.                                                                                                                  |
|                        | 12.2(28)SB     | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                                                                    |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                        | 12.2SX         | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

**Usage Guidelines** You can specify multiple OSPF routing processes in each router.

After you enter the **router ospf** command, you can enter the maximum number of paths. There can be from 1 to 32 paths.

## Examples

The following example configures an OSPF routing process and assign a process number of 109:

```
Router(config)# router ospf 109
```

This example shows a basic OSPF configuration using the **router ospf** command to configure OSPF VRF instance processes for the VRFs first, second, and third:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 12 vrf first
Router(config)# router ospf 13 vrf second
Router(config)# router ospf 14 vrf third
Router(config)# exit
```

The following example shows usage of the **maximum-paths** option:

```
Router> enable
Router# configure terminal
Router(config)# router ospf
Router(config-router)# maximum-paths?
Router(config-router)# 20
Router(config-router)# exit
```

## Related Commands

| Command             | Description                                                                             |
|---------------------|-----------------------------------------------------------------------------------------|
| <b>network area</b> | Defines the interfaces on which OSPF runs and defines the area ID for those interfaces. |

## service (cfm-srv)

To configure a maintenance association within a maintenance domain and place the command-line interface (CLI) into Ethernet connectivity fault management (CFM) service configuration mode (config-ecfm-srv), use the **service** command in Ethernet CFM configuration mode. To remove the configuration, use the **no** form of this command.

**service** {*ma-name* | *ma-num* [**vlan-id** *vlan-id*]}

**no service** {*ma-name* | *ma-num* [**vlan-id** *vlan-id*]}

### Syntax Description

|                |                                                                      |
|----------------|----------------------------------------------------------------------|
| <i>ma-name</i> | Short maintenance association name.                                  |
| <i>ma-num</i>  | Integer from 0 to 65535 that identifies the maintenance association. |
| <b>vlan-id</b> | (Optional) Configures a primary VLAN.                                |
| <i>vlan-id</i> | (Optional) Integer from 1 to 4094 that identifies the primary VLAN.  |

### Command Default

No maintenance associations are configured.

### Command Modes

Ethernet CFM configuration (config-ether-cfm)

### Command History

| Release      | Modification                                                    |
|--------------|-----------------------------------------------------------------|
| 12.2(33)SX12 | This command was introduced.                                    |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

### Usage Guidelines

The maintenance association ID (MAID) is a combination of a maintenance domain ID and the short maintenance association name, and the length of the MAID TLV should not exceed 48 characters.

If you configure the same short maintenance association name for two VLANs in the same domain, an error message is displayed and the command is rejected.

If you specify the service direction as down (outward to the LAN), you can create multiple outward services at the same level containing an overlapping set of VLANs. The set of VLANs in an outward service can also overlap with inward services. A set of VLANs between inward services at the same level must be unique.

### Examples

The following example shows how to configure a maintenance association with the ID 10, VLAN 17, and service direction toward the LAN within the customerA maintenance domain:

```
Router(config)# ethernet cfm domain customerA level 5
Router(config-ether-cfm)# service 10 vlan-id 17 direction down
Router(config-ether-cfm)#
```

# service-policy

To attach a policy map to an input interface, a virtual circuit (VC), an output interface, or a VC that is used as the service policy for the interface or VC, use the **service-policy** command in the appropriate configuration mode. To remove a service policy from an input or output interface or from an input or output VC, use the **no** form of this command.

**service-policy** {**input** | **output**} *policy-map-name*

**no service-policy** {**input** | **output**} *policy-map-name*

|                           |                        |                                                                                                                                                     |
|---------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>input</b>           | Attaches the specified policy map to the input interface or input VC.                                                                               |
|                           | <b>output</b>          | Attaches the specified policy map to the output interface or output VC.                                                                             |
|                           | <i>policy-map-name</i> | Name of a service policy map (created using the <b>policy-map</b> command) to be attached. The name can be a maximum of 40 alphanumeric characters. |

|                        |                                                                                                                |
|------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>Command Default</b> | No service policy is specified.<br>A control policy is not applied to a context.<br>No policy map is attached. |
|------------------------|----------------------------------------------------------------------------------------------------------------|

|                      |                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Command Modes</b> | ATM bundle-VC configuration (config-atm-bundle)<br>ATM PVP configuration (config-if-atm-l2trans-pvp)<br>ATM VC mode (config-if-atm-vc)<br>Global configuration (config)<br>Interface configuration (config-if)<br>Map-class configuration (config-map-class)<br>PVC-in-range configuration (cfg-if-atm-range-pvc)<br>PVC range subinterface configuration (config-subif) |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| <b>Command History</b> | Release      | Modification                                                                                                                   |
|------------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------|
|                        | 12.0(5)T     | This command was introduced.                                                                                                   |
|                        | 12.0(5)XE    | This command was integrated into Cisco IOS Release 12.0(5)XE.                                                                  |
|                        | 12.0(7)S     | This command was integrated into Cisco IOS Release 12.0(7)S.                                                                   |
|                        | 12.0(17)SL   | This command was implemented on the Cisco 10000 series routers.                                                                |
|                        | 12.1(1)E     | This command was integrated into Cisco IOS Release 12.1(1)E.                                                                   |
|                        | 12.1(2)T     | This command was modified to enable low latency queueing (LLQ) on Frame Relay VCs.                                             |
|                        | 12.2(14)SX   | Support for this command was implemented on Cisco 7600 series routers. This command was changed to support output policy maps. |
|                        | 12.2(15)BX   | This command was implemented on the ESR-PRE2.                                                                                  |
|                        | 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.                    |
|                        | 12.2(33)SRA  | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                |

| Release                  | Modification                                                                                                                                                                                                                 |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.4(2)T                 | This command was modified to support PVC range subinterface configuration mode and i PVC-in-range configuration mode to extend policy map functionality on an ATM VC to the ATM VC range.                                    |
| 12.4(4)T                 | The <b>type stack</b> and the <b>type control</b> keywords were added to support flexible packet matching (FPM).                                                                                                             |
| 12.2(28)SB               | This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.                                                                                                              |
| 12.2(31)SB2              | This command was integrated into Cisco IOS Release 12.2(31)SB2.                                                                                                                                                              |
| 12.3(7)XI2               | This command was modified to support PVC range configuration mode and PVC-in-range configuration mode for ATM VCs on the Cisco 10000 series router and the Cisco 7200 series router.                                         |
| 12.2(18)ZY               | The <b>type stack</b> and the <b>type control</b> keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA). |
| 12.2(33)SRC              | Support for this command was enhanced on Cisco 7600 series routers.                                                                                                                                                          |
| 12.2(33)SB               | This command's behavior was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4.                                                                                                                 |
| Cisco IOS XE Release 2.3 | This command was modified to support ATM PVP configuration mode.                                                                                                                                                             |
| 12.4(20)MR               | This command was integrated into Cisco IOS Release 12.4(20)MR. This release does not support the <b>type access-control</b> parameter.                                                                                       |
| 12.2(33)MRA              | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not support the <b>type access-control</b> parameter.                                                                                      |

### Usage Guidelines

Choose the command mode according to the intended use of the command, as follows:

| Application                       | Mode                                 |
|-----------------------------------|--------------------------------------|
| Standalone VC                     | VC submode                           |
| ATM VC bundle members             | Bundle-VC configuration              |
| A range of ATM PVCs               | PVC range subinterface configuration |
| Individual PVC within a PVC range | PVC-in-range configuration           |
| Frame Relay VC                    | Map-class configuration              |

You can attach a single policy map to one or more interfaces or to one or more VCs to specify the service policy for those interfaces or VCs.

A service policy specifies class-based weighted fair queueing (CBWFQ). The class policies that make up the policy map are then applied to packets that satisfy the class map match criteria for the class.

To successfully attach a policy map to an interface or ATM VC, the aggregate of the configured minimum bandwidths of the classes that make up the policy map must be less than or equal to 75 percent of the interface bandwidth or the bandwidth allocated to the VC.



## Examples

The following example shows how to attach a policy map to a Gigabit Ethernet interface:

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/2
Router(config-if)# service-policy input pmap1
```

The following example attaches the service policy map named *policy9* to the output PVC named *mypvc*:

```
Router# configure terminal
Router(config)# pvc mypvc 0/5
Router(config-if-atm-vc)# service-policy output policy9
Router(config-if-atm-vc)# vbr-nt 400 200 500
```

## Related Commands

| Command                          | Description                                                                                                                                                                                  |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>class-map</b>                 | Accesses the QoS class map configuration mode to configure QoS class maps.                                                                                                                   |
| <b>policy-map</b>                | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                                 |
| <b>show policy-map</b>           | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.                                                                    |
| <b>show policy-map interface</b> | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# service-policy (class-map)

To attach a policy map to a class, use the **service-policy** command in class-map configuration mode. To remove a service policy from a class, use the **no** form of this command.

**service-policy** *policy-map*

**no service-policy**

## Syntax Description

|                   |                                                                                                                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>policy-map</i> | Name of a service policy map (created using the <b>policy-map</b> command) to be attached. The name can be a maximum of 40 alphanumeric characters. |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|

## Command Default

No service policy is specified.

## Command Modes

Class-map configuration

## Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.1(2)T    | This command was introduced.                                                                                                                                                      |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

## Usage Guidelines

You can attach a single policy map to one or more classes to specify the service policy for those classes. This command is only available for the output interface, which is assumed.

## Examples

In the following example, three policy maps are defined—cust1-classes, cust2-classes, and cust-policy. The policy maps cust1-classes and cust2-classes have three classes defined—gold, silver, and bronze.

For cust1-classes, gold is configured to use 50 percent of the bandwidth. Silver is configured to use 20 percent of the bandwidth, and bronze is configured to use 15 percent of the bandwidth.

For cust2-classes, gold is configured to use 30 percent of the bandwidth. Silver is configured to use 15 percent of the bandwidth, and bronze is configured to use 10 percent of the bandwidth.

The policy map cust-policy specifies average rate shaping of 384 kbps and assigns the service policy called cust1-classes to the policy map called cust1-classes. The policy map called cust-policy specifies peak rate shaping of 512 kbps and assigns the service policy called cust2-classes to the policy map called cust2-classes.

To configure classes for cust1-classes, use the following commands:

```
Router(config)# policy-map cust1-classes
Router(config-pmap)# class gold
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# exit
Router(config-pmap)# class silver
Router(config-pmap-c)# bandwidth percent 20
Router(config-pmap-c)# exit
Router(config-pmap)# class bronze
Router(config-pmap-c)# bandwidth percent 15
```

To configure classes for cust2, use the following commands:

```
Router(config)# policy-map cust2-classes
Router(config-pmap)# class gold
Router(config-pmap-c)# bandwidth percent 30
Router(config-pmap-c)# exit
Router(config-pmap)# class silver
Router(config-pmap-c)# bandwidth percent 15
Router(config-pmap-c)# exit
Router(config-pmap)# class bronze
Router(config-pmap-c)# bandwidth percent 10
```

To define the customer policy with cust1-classes and cust2-classes and QoS features, use the following commands:

```
Router(config)# policy-map cust-policy
Router(config-pmap)# class cust1
Router(config-pmap-c)# shape average 38400
Router(config-pmap-c)# service-policy cust1-classes
Router(config-pmap-c)# exit
Router(config-pmap)# class cust2
Router(config-pmap-c)# shape peak 51200
Router(config-pmap-c)# service-policy cust2-classes
Router(config-pmap-c)# interface e1 0/2
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# exit
Router(config)# interface e10/0
Router(config-if)# service out cust-policy
```

#### Related Commands

| Command                | Description                                                                                                               |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>policy-map</b>      | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.              |
| <b>show policy-map</b> | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |

# service-policy (policy-map class)

To use a service policy as a QoS policy within a policy map (called a hierarchical service policy), use the **service-policy** command in policy-map class configuration mode. To disable a particular service policy as a QoS policy within a policy map, use the **no** form of this command.

**service-policy** *policy-map-name*

**no service-policy** *policy-map-name*

## Syntax Description

|                        |                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------|
| <i>policy-map-name</i> | Name of the predefined policy map to be used as a QoS policy. The name can be a maximum of 40 alphanumeric characters. |
|------------------------|------------------------------------------------------------------------------------------------------------------------|

## Command Default

No service policies are used.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release                  | Modification                                                                                                                                                                      |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.1(2)E                 | This command was introduced.                                                                                                                                                      |
| 12.1(5)T                 | This command was integrated into Cisco IOS Release 12.1(5)T.                                                                                                                      |
| 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX                   | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers.                                                                                                                    |
| 12.4(20)MR               | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA              | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

## Usage Guidelines

This command is used to create hierarchical service policies in policy-map class configuration mode.

This command is different from the **service-policy** [**input** | **output**] *policy-map-name* command used in interface configuration mode. The purpose of the **service-policy** [**input** | **output**] *policy-map-name* is to attach service policies to interfaces.

The child policy is the previously defined service policy that is being associated with the new service policy through the use of the **service-policy** command. The new service policy using the preexisting service policy is the parent policy.

This command has the following restrictions:

- The **set** command is not supported on the child policy.
- The **priority** command can be used in either the parent or the child policy, but not *both* policies simultaneously.

- The **shape** command can be used in either the parent or the child policy, but not *both* policies simultaneously on a subinterface.
- The **fair-queue** command cannot be defined in the parent policy.
- If the **bandwidth** command is used in the child policy, the **bandwidth** command must also be used in the parent policy. The one exception is for policies using the default class.

### Examples

The following example creates a hierarchical service policy in the service policy called parent:

```
Router(config)# policy-map child
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 500
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# service-policy child
```

### Related Commands

| Command                             | Description                                                                                                                                                                                  |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bandwidth (policy-map class)</b> | Specifies or modifies the bandwidth allocated for a class belonging to a policy map.                                                                                                         |
| <b>fair-queue</b>                   | Specifies the number of queues to be reserved for use by a traffic class.                                                                                                                    |
| <b>policy-map</b>                   | Specifies the name of the service policy to configure.                                                                                                                                       |
| <b>priority</b>                     | Gives priority to a class of traffic belonging to a policy map.                                                                                                                              |
| <b>service-policy</b>               | Specifies the name of the service policy to be attached to the interface.                                                                                                                    |
| <b>shape</b>                        | Specifies average or peak rate traffic shaping.                                                                                                                                              |
| <b>show policy-map</b>              | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.                                                                    |
| <b>show policy-map interface</b>    | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# service-policy type control

To apply a control policy to a context, use the **service-policy type control** command in the appropriate configuration mode. To remove the control policy, use the **no** form of this command.

**service-policy type control** *policy-map-name*

**no service-policy type control** *policy-map-name*

|                           |                        |                                 |
|---------------------------|------------------------|---------------------------------|
| <b>Syntax Description</b> | <i>policy-map-name</i> | Name of the control policy map. |
|---------------------------|------------------------|---------------------------------|

|                        |                                               |
|------------------------|-----------------------------------------------|
| <b>Command Default</b> | A control policy is not applied to a context. |
|------------------------|-----------------------------------------------|

|                      |                                                                                                                                                                       |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Command Modes</b> | Global configuration<br>Interface configuration<br>Subinterface configuration<br>Virtual template configuration<br>ATM VC class configuration<br>ATM VC configuration |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                        |                |                                                                 |
|------------------------|----------------|-----------------------------------------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                             |
|                        | 12.2(28)SB     | This command was introduced.                                    |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                                                                                                                                            |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | A control policy map must be activated by applying it to a context. A control policy map can be applied to one or more of the following types of contexts: |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|

- Global
- Interface
- Subinterface
- Virtual template
- VC class
- PVC

In general, control policy maps that are applied to more specific contexts take precedence over policy maps applied to more general contexts. In the list, the context types are numbered in order of precedence. For example, a control policy map that is applied to a permanent virtual circuit (PVC) takes precedence over a control policy map that is applied to an interface.

Control policies apply to all sessions hosted on the context.

Only one control policy map may be applied to a given context.

---

**Examples**

The following example applies the control policy map “RULEA” to Ethernet interface 0:

```
interface Ethernet 0
 service-policy type control RULEA
```

---

**Related Commands**

| Command                        | Description                                                                    |
|--------------------------------|--------------------------------------------------------------------------------|
| <b>policy-map type control</b> | Creates or modifies a control policy map, which defines an ISG control policy. |

# set atm-clp

To set the cell loss priority (CLP) bit when a policy map is configured, use the **set atm-clp** command in policy-map class configuration mode. To remove a specific CLP bit setting, use the **no** form of this command.

**set atm-clp**

**no set atm-clp**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The CLP bit is automatically set to 0 when Cisco routers convert IP packets into ATM cells for transmission through Multiprotocol Label Switching (MPLS)-aware ATM networks.

## Command Modes

Policy-map class configuration

## Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.1(5)T    | This command was introduced.                                                                                                                                                      |
| 12.2(4)T    | This command was implemented on the Cisco MGX 8850 switch and the MGX 8950 switch with a Cisco MGX RPM-PR card.                                                                   |
| 12.2(4)T2   | This command was implemented on the Cisco 7500 series.                                                                                                                            |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2(31)SB  | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router.                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

## Usage Guidelines

To disable this command, remove the service policy from the interface.

The **set atm-clp** command works only on platforms that support one of the following adapters: the Enhanced ATM Port Adapter (PA-A3), the ATM Inverse Multiplexer over ATM Port Adapter with eight T1 ports (PA-A3-8T1IMA), or the ATM Inverse Multiplexer over ATM Port Adapter with eight E1 ports (PA-A3-8E1IMA). For more information, refer to the documentation for your specific router.

A policy map containing the **set atm-clp** command can be attached as an output policy only. The **set atm-clp** command does not support packets that originate from the router.



## Examples

The following example illustrates setting the CLP bit using the **set atm-clp** command in the policy map:

```
Router(config)# class-map ip-precedence
Router(config-cmap)# match ip precedence 0 1
Router(config-cmap)# exit
Router(config)# policy-map atm-clp-set
Router(config-pmap)# class ip-precedence
Router(config-pmap-c)# set atm-clp
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 1/0/0.1
Router(config-if)# service-policy output policy1
```

## Related Commands

| Command                | Description                                                                                                  |
|------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>policy-map</b>      | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| <b>show atm pvc</b>    | Displays all ATM PVCs and traffic information.                                                               |
| <b>show policy-map</b> | Displays information about the policy map for an interface.                                                  |

# set cos

To set the Layer 2 class of service (CoS) value of an outgoing packet, use the **set cos** command in policy-map class configuration mode. To remove a specific CoS value setting, use the **no** form of this command.

**set cos** {*cos-value*}

**no set cos** {*cos-value*}

|                           |                  |                                             |
|---------------------------|------------------|---------------------------------------------|
| <b>Syntax Description</b> | <i>cos-value</i> | Specific IEEE 802.1Q CoS value from 0 to 7. |
|---------------------------|------------------|---------------------------------------------|

|                        |                                              |
|------------------------|----------------------------------------------|
| <b>Command Default</b> | No CoS value is set for the outgoing packet. |
|------------------------|----------------------------------------------|

|                      |                                |
|----------------------|--------------------------------|
| <b>Command Modes</b> | Policy-map class configuration |
|----------------------|--------------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                                                               |
|------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | 12.1(5)T       | This command was introduced.                                                                                                                                                      |
|                        | 12.2(13)T      | This command was modified for Enhanced Packet Marking to allow a mapping table (table map) to be used to convert and propagate packet-marking values.                             |
|                        | 12.0(16)BX     | This command was implemented on the Cisco 10000 series router for the ESR-PRE2.                                                                                                   |
|                        | 12.0(31)S      | This command was integrated into Cisco IOS Release 12.0(31)S.                                                                                                                     |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                        | 12.2(31)SB     | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router.                                                                   |
|                        | 12.2SX         | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR. This release does not support the <i>from-field</i> or <b>table</b> options.                                       |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not support the <i>from-field</i> or <b>table</b> options.                                      |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | <p>CoS packet marking is supported only in the Cisco Express Forwarding switching path.</p> <p>The <b>set cos</b> command should be used by a router if a user wants to mark a packet that is being sent to a switch. Switches can leverage Layer 2 header information, including a CoS value marking.</p> <p>The <b>set cos</b> command can be used only in service policies that are attached in the output direction of an interface. Packets entering an interface cannot be set with a CoS value.</p> |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

The **match cos** and **set cos** commands can be used together to allow routers and switches to interoperate and provide quality of service (QoS) based on the CoS markings.

Layer 2 to Layer 3 mapping can be configured by matching on the CoS value because switches already can match and set CoS values. If a packet that needs to be marked to differentiate user-defined QoS services is leaving a router and entering a switch, the router should set the CoS value of the packet because the switch can process the Layer 2 header.

#### Using This Command with the Enhanced Packet Marking Feature

You can use this command as part of the Enhanced Packet Marking feature—to specify the from-field packet-marking category to be used for mapping and setting the CoS value. The from-field packet-marking categories are as follows:

- Precedence
- Differentiated services code point (DSCP)

If you specify a from-field category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action is to copy the value associated with the from-field category as the CoS value. For instance, if you configure the **set cos precedence** command, the precedence value is copied and used as the CoS value.

You can do the same for the DSCP marking category. That is, you can configure the **set cos dscp** command, and the DSCP value is copied and used as the CoS value.



#### Note

If you configure the **set cos dscp** command, only the *first three bits* (the class selector bits) of the DSCP field are used.

## Examples

In the following example, the policy map called *cos-set* is created to assign different CoS values for different types of traffic. This example assumes that the class maps called *voice* and *video-data* have already been created.

```
Router(config)# policy-map cos-set
Router(config-pmap)# class voice
Router(config-pmap-c)# set cos 1
Router(config-pmap-c)# exit
Router(config-pmap)# class video-data
Router(config-pmap-c)# set cos 2
Router(config-pmap-c)# end
```

#### Enhanced Packet Marking Example

In the following example, the policy map called *policy-cos* is created to use the values defined in a table map called *table-map1*. The table map called *table-map1* was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

In this example, the setting of the CoS value is based on the precedence value defined in table-map:

```
Router(config)# policy-map policy-cos
Router(config-pmap)# class class-default
Router(config-pmap-c)# set cos precedence table table-map1
Router(config-pmap-c)# end
```

**Note**

The **set cos** command is applied when you create a service policy in QoS policy-map configuration mode and attach the service policy to an interface or ATM virtual circuit (VC). For information on attaching a service policy, refer to the “Modular Quality of Service Command-Line Interface Overview” chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

**Related Commands**

| Command                          | Description                                                                                                                                                                                  |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>match cos</b>                 | Matches a packet on the basis of Layer 2 CoS marking.                                                                                                                                        |
| <b>policy-map</b>                | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                                 |
| <b>service-policy</b>            | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.                                                  |
| <b>set dscp</b>                  | Marks a packet by setting the Layer 3 DSCP value in the ToS byte.                                                                                                                            |
| <b>set precedence</b>            | Sets the precedence value in the packet header.                                                                                                                                              |
| <b>show policy-map</b>           | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.                                                                    |
| <b>show policy-map class</b>     | Displays the configuration for the specified class of the specified policy map.                                                                                                              |
| <b>show policy-map interface</b> | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

## set cos-inner

To mark the inner class of service field in a bridged frame, use the **set cos-inner** command in policy-map class configuration mode. To remove marking of the inner CoS field, use the **no** form of this command.

**set cos-inner** *cos-value*

**no set cos-inner** *cos-value*

### Syntax Description

|                  |                                    |
|------------------|------------------------------------|
| <i>cos-value</i> | IEEE 802.1q CoS value from 0 to 7. |
|------------------|------------------------------------|

### Command Default

No default behavior or values.

### Command Modes

Policy-map class configuration

### Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(33)SRA | This command was introduced.                                    |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

### Usage Guidelines

This command was introduced in Cisco IOS Release 12.2(33)SRA to support marking of the inner CoS value when using multipoint bridging (MPB) features on the Enhanced FlexWAN module, and when using MPB features on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router.

This command is not supported on the Cisco 7600 SIP-600.

On the Cisco 7600 SIP-200, this command is not supported with the **set cos** command on the same interface.

For more information about QoS and the forms of marking commands supported by the SIPs on the Cisco 7600 series router, refer to the *Cisco 7600 Series SIP, SSC, and SPA Software Configuration Guide*.

### Examples

The following example shows configuration of a QoS class that filters all traffic matching on VLAN 100 into a class named “vlan-inner-100.” The configuration shows the definition of a policy-map (also named “vlan-inner-100”) that marks the inner CoS with a value of 3 for traffic in the vlan-inner-100 class. Since marking of the inner CoS value is only supported with bridging features, the configuration also shows the service policy being applied as an output policy to a serial SPA interface that bridges traffic into VLAN 100 using the **bridge-domain** command:

```
Router(config)# class-map match-all vlan-inner-100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
Router(config)# policy-map vlan-inner-100
Router(config-pmap)# class vlan-inner-100
```

```

Router(config-pmap-c)# set cos-inner 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/0/0
Router(config-if)# no ip address
Router(config-if)# encapsulation ppp
Router(config-if)# bridge-domain 100 dot1q
Router(config-if)# service-policy output vlan-inner-100
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# end

```

**Related Commands**

| Command                   | Description                                                                                                                                                                                         |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bridge-domain</b>      | Enables RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged virtual LAN (VLAN) to an ATM permanent virtual circuit (PVC) or Frame Relay data-link connection identifier (DLCI). |
| <b>class-map</b>          | Creates a class map to be used for matching packets to a specified class.                                                                                                                           |
| <b>class (policy-map)</b> | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.                       |
| <b>policy-map</b>         | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                                        |
| <b>service-policy</b>     | Attaches a policy map to an input interface or virtual circuit (VC) or an output interface or VC, to be used as the service policy for that interface or VC.                                        |

# set cos-inner cos

To copy the outer COS to the inner COS for double-tagged packets, use the **set cos-inner cos** command in policy-map class configuration mode. To remove the outer COS copied to the inner COS for double-tagged packets, use the **no** form of this command.

**set cos-inner cos** *cos-value*

**no set cos-inner cos** *cos-value*

|                           |                  |                                    |
|---------------------------|------------------|------------------------------------|
| <b>Syntax Description</b> | <i>cos-value</i> | IEEE 802.1q CoS value from 0 to 7. |
|---------------------------|------------------|------------------------------------|

|                        |                                |
|------------------------|--------------------------------|
| <b>Command Default</b> | No default behavior or values. |
|------------------------|--------------------------------|

|                      |                                |
|----------------------|--------------------------------|
| <b>Command Modes</b> | Policy-map class configuration |
|----------------------|--------------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                             |
|------------------------|----------------|-----------------------------------------------------------------|
|                        | 12.2(33)SRB    | This command was introduced.                                    |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                                                                                                                                                                                                                                 |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | This command was introduced in Cisco IOS Release 12.2(33)SRB and is limited to policies that are applied to the EVC service instances.                                                                                                          |
|                         | For classification, the reference to the outer and inner tags is made to the frames as seen on the wire - that is, for ingress frames, tags prior to the rewrite, while the for egress, it is after the rewrite of the tags, if any.            |
|                         | For marking, the reference to the outer COS at the ingress is to the DBUS-COS and reference to the inner is to the COS in the first tag on the frame; whereas, at the egress, the reference to outer and inner COS is to the ones in the frame. |

|                 |                                                                                               |
|-----------------|-----------------------------------------------------------------------------------------------|
| <b>Examples</b> | The following example matches on outer COS 3 and 4 and copies the outer COS to the inner COS. |
|-----------------|-----------------------------------------------------------------------------------------------|

```
Router(config)# class-map cos3_4
Router(config-cmap)# match cos 3 4
Router(config)# policy-map mark-it-in
Router(config-pmap)# class cos3_4
Router(config-pmap-c)# set cos-inner cos
```

| Related Commands | Command                   | Description                                                                                                                                                                                         |
|------------------|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>bridge-domain</b>      | Enables RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged virtual LAN (VLAN) to an ATM permanent virtual circuit (PVC) or Frame Relay data-link connection identifier (DLCI). |
|                  | <b>class-map</b>          | Creates a class map to be used for matching packets to a specified class.                                                                                                                           |
|                  | <b>class (policy-map)</b> | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.                       |
|                  | <b>policy-map</b>         | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                                        |
|                  | <b>service-policy</b>     | Attaches a policy map to an input interface or virtual circuit (VC) or an output interface or VC, to be used as the service policy for that interface or VC.                                        |



# set discard-class

To mark a packet with a discard-class value, use the **set discard-class** command in QoS policy-map configuration mode. To prevent the discard-class value of a packet from being altered, use the **no** form of this command.

**set discard-class** *value*

**no set discard-class** *value*

## Syntax Description

|              |                                                                                                                                                |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>value</i> | Specifies per-hop behavior (PHB) for dropping traffic. The value sets the priority of a type of traffic. Valid values are numbers from 0 to 7. |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------|

## Command Default

If you do not enter this command, the packet has a discard-class value of 0.

## Command Modes

QoS policy-map configuration

## Command History

| Release     | Modification                                                                    |
|-------------|---------------------------------------------------------------------------------|
| 12.2(13)T   | This command was introduced.                                                    |
| 12.3(7)XI   | This command was implemented on the Cisco 10000 series router for the ESR-PRE2. |
| 12.2(31)SB  | This command was integrated into Cisco IOS Release 12.2(31)SB.                  |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                 |

## Usage Guidelines

The discard class value indicates the discard portion of the PHB. Use the **set discard-class** command only in DiffServ Tunneling Pipe mode. The discard class value is required when the input PHB marking is used to classify packets on the output interface.

You can also use this command to specify the type of traffic that is dropped when there is congestion.

## Examples

The following example shows that traffic is set to the discard-class value of 2:

```
set discard-class 2
```

| Related Commands | Command                    | Description                                        |
|------------------|----------------------------|----------------------------------------------------|
|                  | <b>match discard-class</b> | Matches packets of a certain discard class.        |
|                  | <b>random-detect</b>       | Bases WRED on the discard class value of a packet. |
|                  | <b>discard-class-based</b> |                                                    |

# set dscp

To mark a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte, use the **set dscp** command in policy-map class configuration mode. To remove a previously set DSCP value, use the **no** form of this command.

**set [ip] dscp** {*dscp-value*}

**no set [ip] dscp** {*dscp-value*}

|                           |                   |                                                                                                                                                                                                                                                                                                                            |
|---------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>ip</b>         | (Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets.                                                                                                                                                                                                     |
|                           | <i>dscp-value</i> | A number from 0 to 63 that sets the DSCP value. The following reserved keywords can be specified instead of numeric values: <ul style="list-style-type: none"><li>• <b>EF</b> (expedited forwarding)</li><li>• <b>AF11</b> (assured forwarding class AF11)</li><li>• <b>AF12</b> (assured forwarding class AF12)</li></ul> |

|                        |          |
|------------------------|----------|
| <b>Command Default</b> | Disabled |
|------------------------|----------|

|                      |                                |
|----------------------|--------------------------------|
| <b>Command Modes</b> | Policy-map class configuration |
|----------------------|--------------------------------|

|                        |                |                                                                                                                                               |
|------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                           |
|                        | 12.2(13)T      | This command was introduced. It replaces the <b>set ip dscp</b> command.                                                                      |
|                        | 12.0(28)S      | Support for this command in IPv6 was added on the in Cisco IOS Release 12.0(28)S                                                              |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR. This release does not support the <i>from-field</i> and <b>table</b> options.  |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not support the <i>from-field</i> and <b>table</b> options. |

**Usage Guidelines**

Once the DSCP bit is set, other quality of service (QoS) features can then operate on the bit settings.

**DSCP and Precedence Values Are Mutually Exclusive**

The **set dscp** command cannot be used with the **set precedence** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

**Precedence Value and Queueing**

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

**Use of the “from-field” Packet-marking Category**

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the “from-field” packet-marking category to be used for mapping and setting the DSCP value. The “from-field” packet-marking categories are as follows:

- Class of service (CoS)
- QoS group

If you specify a “from-field” category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action is to copy the value associated with the “from-field” category as the DSCP value. For instance, if you configure the **set dscp cos** command, the CoS value is copied and used as the DSCP value.

**Note**

The CoS field is a three-bit field, and the DSCP field is a six-bit field. If you configure the **set dscp cos** command, only the three bits of the CoS field are used.

If you configure the **set dscp qos-group** command, the QoS group value is copied and used as the DSCP value.

The valid value range for the DSCP is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set dscp qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value is copied and the packets are marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value is not copied and the packet is not marked. No action is taken.

**Set DSCP Values in IPv6 Environments**

When this command is used in IPv6 environments, the default match occurs on both IP and IPv6 packets. However, the actual packets set by this function are only those which meet the match criteria of the class-map containing this function.

**Set DSCP Values for IPv6 Packets Only**

To set DSCP values for IPv6 values only, the **match protocol ipv6** command must also be used. Without that command, the precedence match defaults to match both IPv4 and IPv6 packets.

**Set DSCP Values for IPv4 Packets Only**

To set DSCP values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword, the match occurs on both IPv4 and IPv6 packets.

**Examples****Packet-marking Values and Table Map**

In the following example, the policy map called “policy1” is created to use the packet-marking values defined in a table map called “table-map1”. The table map was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the table-map (value mapping) command page.

In this example, the DSCP value is set according to the CoS value defined in the table map called “table-map1”.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set dscp cos table table-map1
Router(config-pmap-c)# end
```

The **set dscp** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface. For information on attaching a service policy to an interface, refer to the “Modular Quality of Service Command-Line Interface” section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

**Related Commands**

| Command                          | Description                                                                                                                                                                                  |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>match protocol</b>            | Configures the match criteria for a class map on the basis of the specified protocol.                                                                                                        |
| <b>policy-map</b>                | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                                 |
| <b>service-policy</b>            | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.                                                  |
| <b>set cos</b>                   | Sets the Layer 2 CoS value of an outgoing packet.                                                                                                                                            |
| <b>set precedence</b>            | Sets the precedence value in the packet header.                                                                                                                                              |
| <b>show policy-map</b>           | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.                                                                    |
| <b>show policy-map class</b>     | Displays the configuration for the specified class of the specified policy map.                                                                                                              |
| <b>show policy-map interface</b> | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |
| <b>show table-map</b>            | Displays the configuration of a specified table map or all table maps.                                                                                                                       |
| <b>table-map (value mapping)</b> | Creates and configures a mapping table for mapping and converting one packet-marking value to another.                                                                                       |

# set fr-de

To change the discard eligible (DE) bit setting in the address field of a Frame Relay frame to 1 for all traffic leaving an interface, use the **set fr-de** command in policy-map class command. To remove the DE bit setting, use the **no** form of this command.

**set fr-de**

**no set fr-de**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The DE bit is usually set to 0. This command changes the DE bit setting to 1.

**Command Modes** Policy-map class

| Command History | Release     | Modification                                                                                                                |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------|
|                 | 12.2(2)T    | This command was introduced.                                                                                                |
|                 | 12.2(31)SB2 | This command was integrated in Cisco IOS Release 12.2(31)SB2, and introduced on the PRE3 for the Cisco 10000 series router. |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                              |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                             |

**Usage Guidelines** To disable this command in a traffic policy, use the **no set fr-de** command in policy-map class configuration mode of the traffic policy.

If the DE bit is already set to 1, no changes are made to the frame.

**Examples** The following example shows how to set the DE bit using the **set fr-de** command in the traffic policy. The router sets the DE bit of outbound packets belonging to the ip-precedence class.

```
Router(config)# class-map ip-precedence
Router(config-cmap)# match ip precedence 0 1
Router(config-cmap)# exit
Router(config)# policy-map set-de
Router(config-pmap)# class ip-precedence
Router(config-pmap-c)# set fr-de
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial 1/0/0
Router(config-if)# no ip address
Router(config-if)# encapsulation frame-relay
Router(config-if)# interface serial 1/0/0.1
Router(config-subif)# ip address 10.1.1.1 255.255.255.252
Router(config-subif)# no ip directed-broadcast
Router(config-subif)# service-policy output set-de
```

| Related Commands | Command                | Description                                                                                                               |
|------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------|
|                  | <b>policy-map</b>      | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.              |
|                  | <b>show policy-map</b> | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |

## set ip dscp

The **set ip dscp** command is replaced by the [set dscp](#) command. See the [set dscp](#) command for more information.



# set ip dscp (policy-map configuration)

To mark a packet by setting the IP differentiated services code point (DSCP) value in the type of service (ToS) byte, use the **set ip dscp** command in policy-map configuration mode. To remove a previously set IP DSCP value, use the **no** form of this command.

**set ip dscp** *ip-dscp-value*

**no set ip dscp** *ip-dscp-value*

|                           |                      |                                                                                                              |
|---------------------------|----------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>ip-dscp-value</i> | IP DSCP value; valid values are from 0 to 63. See the “Usage Guidelines” section for additional information. |
|---------------------------|----------------------|--------------------------------------------------------------------------------------------------------------|

|                        |                                       |
|------------------------|---------------------------------------|
| <b>Command Default</b> | This command has no default settings. |
|------------------------|---------------------------------------|

|                      |                          |
|----------------------|--------------------------|
| <b>Command Modes</b> | Policy-map configuration |
|----------------------|--------------------------|

|                        |                |                                                                                                             |
|------------------------|----------------|-------------------------------------------------------------------------------------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                         |
|                        | 12.2(14)SX     | Support for this command was introduced on the Supervisor Engine 720.                                       |
|                        | 12.2(17d)SXB   | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                             |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.                                              |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                             |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | You can enter reserved keywords <b>EF</b> (expedited forwarding), <b>AF11</b> (assured forwarding class AF11), and <b>AF12</b> (assured forwarding class AF12) instead of numeric values for <i>ip-dscp-value</i> .                                                                                                                                                                                                                                                    |
|                         | After the IP DSCP bit is set, other quality of service (QoS) features can operate on the bit settings.                                                                                                                                                                                                                                                                                                                                                                 |
|                         | You cannot mark a packet by the IP precedence using the <b>set ip precedence</b> (policy-map configuration) command and then mark the same packet with an IP DSCP value using the <b>set ip dscp</b> command.                                                                                                                                                                                                                                                          |
|                         | The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set IP precedence at the edge of the network (or administrative domain); data is queued based on the precedence. Weighted Fair Queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) ensures that high-precedence traffic has lower loss rates than other traffic during traffic congestion. |
|                         | The <b>set ip precedence</b> (policy-map configuration) command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not attached to an interface or to an ATM virtual circuit. See the <b>service-policy</b> command for information on attaching a service policy to an interface.                                                                                                                               |

When configuring policy-map class actions, note the following:

- For hardware-switched traffic, Policy Feature Card (PFC) QoS does not support the **bandwidth**, **priority**, **queue-limit**, or **random-detect** policy-map class commands. You can configure these commands because they can be used for software-switched traffic.
- PFC QoS does not support the **set mpls** or **set qos-group** policy-map class commands.
- PFC QoS supports the **set ip dscp** and **set ip precedence** policy-map class commands (see the “Configuring Policy Map Class Marking” section in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*).
- You cannot do all three of the following in a policy-map class:
  - Mark traffic with the **set ip dscp** or **set ip precedence** (policy-map configuration) commands
  - Configure the trust state
  - Configure policing
- In a policy-map class, you can either mark traffic with the **set ip dscp** or **set ip precedence** (policy-map configuration) commands or do one or both of the following:
  - Configure the trust state
  - Configure policing

## Examples

This example shows how to set the IP DSCP ToS byte to 8 in the policy map called policy1:

```
Router(config)# policy-map policy1
Router(config-cmap)# class class1
Router(config-cmap)# set ip dscp 8
```

All packets that satisfy the match criteria of class1 are marked with the IP DSCP value of 8. How packets that are marked with the IP DSCP value of 8 are treated is determined by the network configuration.

This example shows that after you configure the settings that are shown for voice packets at the edge of the network, all intermediate routers are then configured to provide low-latency treatment to the voice packets:

```
Router(config)# class-map voice
Router(config-cmap)# match ip dscp ef
Router(config)# policy qos-policy
Router(config-cmap)# class voice
Router(config-cmap)# priority 24
```

## Related Commands

| Command                          | Description                                                                                                        |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>policy-map</b>                | Accesses QoS policy-map configuration mode to configure the QoS policy map.                                        |
| <b>service-policy</b>            | Attaches a policy map to an interface.                                                                             |
| <b>show policy-map</b>           | Displays information about the policy map.                                                                         |
| <b>show policy-map interface</b> | Displays the statistics and the configurations of the input and output policies that are attached to an interface. |

# set ip dscp tunnel

To set the differentiated services code point (DSCP) value in the tunnel header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) or Generic Routing Encapsulation (GRE) tunneled packet for tunnel marking, use the **set ip dscp tunnel** command in policy-map class configuration mode. To disable this functionality, use the **no** form of this command.

**set ip dscp tunnel** *dscp-value*

**no set ip dscp tunnel** *dscp-value*

|                           |                   |                                                                                                                                                                                                                                                                                  |
|---------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>dscp-value</i> | Number from 0 to 63 that identifies the tunnel header value. The following reserved keywords can be specified instead of numeric values: <ul style="list-style-type: none"> <li><b>EF</b> (expedited forwarding)</li> <li><b>AF11</b> (assured forwarding class AF11)</li> </ul> |
|---------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                        |                            |
|------------------------|----------------------------|
| <b>Command Default</b> | The DSCP value is not set. |
|------------------------|----------------------------|

|                      |                                                |
|----------------------|------------------------------------------------|
| <b>Command Modes</b> | Policy-map class configuration (config-pmap-c) |
|----------------------|------------------------------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                                                                                                                                                                   |
|------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | 12.0(28)S      | This command was introduced.                                                                                                                                                                                                                                                          |
|                        | 12.2(28)SB     | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                                                                                                                                                                        |
|                        | 12.2(33)SRC    | This command was integrated into Cisco IOS Release 12.2(33)SRC.                                                                                                                                                                                                                       |
|                        | 12.4(15)T2     | This command was integrated into Cisco IOS Release 12.4(15)T2, and support for marking GRE-tunneled packets was included. <p><b>Note</b> For this release, marking GRE-tunneled packets is supported only on platforms equipped with a Cisco MGX Route Processor Module (RPM-XF).</p> |
|                        | 12.2(33)SB     | Support for marking GRE-tunneled packets was included, and support for the Cisco 7300 series router was added.                                                                                                                                                                        |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                                                                                                                        |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                                                                                                                       |

**Usage Guidelines**

It is possible to configure L2TPv3 (or GRE) tunnel marking and the **ip tos** command at the same time. However, Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) (L2TPv3 or GRE) tunnel marking has higher priority over **ip tos** commands, meaning that tunnel marking always rewrites the IP header of the tunnel packet and overwrites the values set by **ip tos** commands. The order of enforcement is as follows when these commands are used simultaneously:

1. **set ip dscp tunnel** or **set ip precedence tunnel** (L2TPv3 or GRE tunnel marking)
2. **ip tos reflect**
3. **ip tos tos-value**

This is the designed behavior. We recommend that you configure only L2TPv3 (or GRE) tunnel marking and reconfigure any peers configured with the **ip tos** command to use L2TPv3 (or GRE) tunnel marking.

**Note**

For Cisco IOS Release 12.4(15)T2, marking GRE-tunneled packets is supported only on platforms equipped with a Cisco RPM-XF.

**Examples**

The following example shows the **set ip dscp tunnel** command used in a tunnel marking configuration. In this example, a class map called “class-cl” has been configured to match traffic on the basis of the Frame Relay discard eligible (DE) bit setting. Also, a policy map called “policy1” has been created within which the **set ip dscp tunnel** command has been configured.

```
Router> enable
Router# configure terminal
Router(config)# class-map class-cl
Router(config-cmap)# match fr-de
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class tunnel
Router(config-pmap-c)# set ip dscp tunnel 5
Router(config-pmap-c)# end
```

**Note**

You must still attach a policy map to an interface or ATM PVC using the **service-policy** command. Policy maps with this tunnel marking are not accepted in the output direction. For more information about attaching a policy map to an interface or ATM PVC, see the “Applying QoS Features Using the MQC” module of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

**Related Commands**

| Command                         | Description                                                                  |
|---------------------------------|------------------------------------------------------------------------------|
| <b>ip tos</b>                   | Specifies the ToS level for IP traffic.                                      |
| <b>set ip precedence tunnel</b> | Sets the precedence value in the header of an L2TPv3 or GRE tunneled packet. |

# set ip precedence (policy-map configuration)

To set the precedence value in the IP header, use the **set ip precedence** command in policy-map configuration mode. To leave the precedence value at the current setting, use the **no** form of this command.

**set ip precedence** *ip-precedence-value*

**no set ip precedence**

## Syntax Description

*ip-precedence-value* Precedence-bit value in the IP header; valid values are from 0 to 7. See [Table 13](#) for a list of value definitions.

## Command Default

This command is disabled by default.

## Command Modes

Policy-map configuration

## Command History

| Release      | Modification                                                                                                |
|--------------|-------------------------------------------------------------------------------------------------------------|
| 12.2(14)SX   | Support for this command was introduced on the Supervisor Engine 720.                                       |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA  | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                             |
| 12.4(20)MR   | This command was integrated into Cisco IOS Release 12.4(20)MR.                                              |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                             |

## Usage Guidelines

[Table 13](#) lists the value definitions for precedence values in the IP header. They are listed from least to most important.

**Table 13 Value Definitions for IP Precedence**

| Values | Definitions    |
|--------|----------------|
| 0      | routine        |
| 1      | priority       |
| 2      | immediate      |
| 3      | flash          |
| 4      | flash-override |
| 5      | critical       |
| 6      | internet       |
| 7      | network        |

After the IP precedence bits are set, other quality of service (QoS) features, such as Weighted Fair Queueing (WFQ) and Weighted Random Early Detection (WRED), operate on the bit settings.

The network priorities (or some type of expedited handling) mark traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set IP precedence at the edge of the network (or administrative domain); data is queued based on the precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during traffic congestion.

The **set ip precedence** command is applied when you create a service policy in policy-map configuration mode. This service policy is not attached to an interface or to an ATM virtual circuit. See the **service-policy** command for information on attaching a service policy to an interface.

### Examples

This example shows how to set the IP precedence to 5 for packets that satisfy the match criteria of the class map called class1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip precedence 5
```

All packets that satisfy the match criteria of class1 are marked with the IP precedence value of 5. How packets that are marked with the IP-precedence value of 5 are treated is determined by the network configuration.

### Related Commands

| Command                          | Description                                                                                                        |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>policy-map</b>                | Accesses QoS policy-map configuration mode to configure the QoS policy map.                                        |
| <b>service-policy</b>            | Attaches a policy map to an interface.                                                                             |
| <b>show policy-map</b>           | Displays information about the policy map.                                                                         |
| <b>show policy-map interface</b> | Displays the statistics and the configurations of the input and output policies that are attached to an interface. |

## set ip precedence (policy-map)

The **set ip precedence** (policy-map) command is replaced by the **set precedence** command. See the **set precedence** command for more information.

## set ip precedence (route-map)

To set the precedence value (and an optional IP number or IP name) in the IP header, use the **set ip precedence** command in route-map configuration mode. To leave the precedence value unchanged, use the **no** form of this command.

**set ip precedence** [*number* | *name*]

**no set ip precedence**

### Syntax Description

*number* | *name* (Optional) A number or name that sets the precedence bits in the IP header. The values for the *number* argument and the corresponding *name* argument are listed in [Table 14](#) from least to most important.

### Command Default

Disabled

### Command Modes

Route-map configuration

### Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.0        | This command was introduced.                                                                                                                                                      |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

### Usage Guidelines

[Table 14](#) lists the values for the *number* argument and the corresponding *name* argument for precedence values in the IP header. They are listed from least to most important.

**Table 14**      *Number and Name Values for IP Precedence*

| Number | Name                  |
|--------|-----------------------|
| 0      | <b>routine</b>        |
| 1      | <b>priority</b>       |
| 2      | <b>immediate</b>      |
| 3      | <b>flash</b>          |
| 4      | <b>flash-override</b> |
| 5      | <b>critical</b>       |



**Table 14**      **Number and Name Values for IP Precedence**

|   |                 |
|---|-----------------|
| 6 | <b>internet</b> |
| 7 | <b>network</b>  |

You can set the precedence using either a number or the corresponding name. Once the IP Precedence bits are set, other QoS services such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

The network gives priority (or some type of expedited handling) to marked traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set IP Precedence at the edge of the network (or administrative domain); data then is queued based on the precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during times of congestion.

The mapping from arguments such as **routine** and **priority** to a precedence value is useful only in some instances. That is, the use of the precedence bit is evolving. You can define the meaning of a precedence value by enabling other features that use the value. In the case of the high-end Internet QoS available from Cisco, IP Precedences can be used to establish classes of service that do not necessarily correspond numerically to better or worse handling in the network.

Use the **route-map** (IP) global configuration command with the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another, or for policy routing. Each **route-map** command has an associated list of **match** and **set** commands. The **match** commands specify the match criteria—the conditions under which redistribution or policy routing is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution or policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution set actions to be performed when all of the match criteria of a route map are met.

## Examples

The following example sets the IP Precedence to 5 (critical) for packets that pass the route map match:

```
interface serial 0
 ip policy route-map texas

route-map texas
match length 68 128
set ip precedence 5
```

## Related Commands

| Command                   | Description                                                           |
|---------------------------|-----------------------------------------------------------------------|
| <b>random-detect dscp</b> | Changes the minimum and maximum packet thresholds for the DSCP value. |

# set ip precedence tunnel

To set the precedence value in the header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) or Generic Routing Encapsulation (GRE) tunneled packet for tunnel marking, use the **set ip precedence tunnel** command in policy-map class configuration mode. To disable this functionality, use the **no** form of this command.

**set ip precedence tunnel** *precedence-value*

**no set ip precedence tunnel** *precedence-value*

|                           |                         |                                                                               |
|---------------------------|-------------------------|-------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>precedence-value</i> | Number from 0 to 7 that identifies the precedence value of the tunnel header. |
|---------------------------|-------------------------|-------------------------------------------------------------------------------|

|                        |                                  |
|------------------------|----------------------------------|
| <b>Command Default</b> | The precedence value is not set. |
|------------------------|----------------------------------|

|                      |                                                |
|----------------------|------------------------------------------------|
| <b>Command Modes</b> | Policy-map class configuration (config-pmap-c) |
|----------------------|------------------------------------------------|

| Command History | Release     | Modification                                                                                                                                         |
|-----------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.0(28)S   | This command was introduced.                                                                                                                         |
|                 | 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                                       |
|                 | 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC.                                                                                      |
|                 | 12.4(15)T2  | This command was integrated into Cisco IOS Release 12.4(15)T2, and support for marking GRE-tunneled packets was included.                            |
|                 |             | <b>Note</b> For this release, marking GRE-tunneled packets is supported only on platforms equipped with a Cisco MGX Route Processor Module (RPM-XF). |
|                 | 12.2(33)SB  | Support for marking GRE-tunneled packets was included, and support for the Cisco 7300 series router was added.                                       |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                       |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                      |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | It is possible to configure L2TPv3 (or GRE) tunnel marking and the <b>ip tos</b> command at the same time. However, Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) (L2TPv3 or GRE) tunnel marking has higher priority over <b>ip tos</b> commands, meaning that tunnel marking always rewrites the IP header of the tunnel packet and overwrites the values set by <b>ip tos</b> commands. The order of enforcement is as follows when these commands are used simultaneously: |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

1. **set ip dscp tunnel** or **set ip precedence tunnel** (L2TPv3 or GRE tunnel marking)
2. **ip tos reflect**
3. **ip tos tos-value**

This is the designed behavior. We recommend that you configure only L2TPv3 (or GRE) tunnel marking and reconfigure any peers configured with the **ip tos** command to use L2TPv3 (or GRE) tunnel marking.

**Note**

For Cisco IOS Release 12.4(15)T2, marking GRE-tunneled packets is supported only on platforms equipped with a Cisco RPM-XF.

**Examples**

The following example shows the **set ip precedence tunnel** command used in a tunnel marking configuration. In this example, a class map called “MATCH\_FRDE” has been configured to match traffic on the basis of the Frame Relay discard eligible (DE) bit setting. Also, a policy map called “policy1” has been created within which the **set ip precedence tunnel** command has been configured.

```
Router> enable
Router# configure terminal
Router(config)# class-map MATCH_FRDE
Router(config-cmap)# match fr-de
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class tunnel
Router(config-pmap-c)# set ip precedence tunnel 7
Router(config-pmap-c)# end
```

**Note**

You must still attach a policy map to an interface or ATM PVC using the **service-policy** command. Policy maps with this tunnel marking are not accepted in the output direction. For more information about attaching a policy map to an interface or ATM PVC, see the “Applying QoS Features Using the MQC” module of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

**Related Commands**

| Command                   | Description                                                     |
|---------------------------|-----------------------------------------------------------------|
| <b>ip tos</b>             | Specifies the ToS level for IP traffic in the TN3270 server.    |
| <b>set ip dscp tunnel</b> | Sets the DSCP value in the header of an L2TPv3 tunneled packet. |

## set ip tos (route-map)

To set the type of service (ToS) bits in the header of an IP packet, use the **set ip tos** command in route-map configuration mode. To leave the ToS bits unchanged, use the **no** form of this command.

**set ip tos** [*tos-bit-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**]

**no set ip tos**

### Syntax Description

|                          |                                                                                                                                      |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <i>tos-bit-value</i>     | (Optional) A value (number) from 0 to 15 that sets the ToS bits in the IP header. See <a href="#">Table 15</a> for more information. |
| <b>max-reliability</b>   | (Optional) Sets the maximum reliability ToS bits to 2.                                                                               |
| <b>max-throughput</b>    | (Optional) Sets the maximum throughput ToS bits to 4.                                                                                |
| <b>min-delay</b>         | (Optional) Sets the minimum delay ToS bits to 8.                                                                                     |
| <b>min-monetary-cost</b> | (Optional) Sets the minimum monetary cost ToS bits to 1.                                                                             |
| <b>normal</b>            | (Optional) Sets the normal ToS bits to 0.                                                                                            |

### Command Default

Disabled

### Command Modes

Route-map configuration

### Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.2        | This command was introduced.                                                                                                                                                      |
| 12.4T       | This command was integrated into Cisco IOS Release 12.4T.                                                                                                                         |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

### Usage Guidelines

This command allows you to set four bits in the ToS byte header. [Table 15](#) shows the format of the four bits in binary form.

**Table 15 ToS Bits and Description**

| T3 | T2 | T1 | T0 | Description             |
|----|----|----|----|-------------------------|
| 0  | 0  | 0  | 0  | 0 normal forwarding     |
| 0  | 0  | 0  | 1  | 1 minimum monetary cost |
| 0  | 0  | 1  | 0  | 2 maximum reliability   |

**Table 15** ToS Bits and Description (continued)

|   |   |   |   |                      |
|---|---|---|---|----------------------|
| 0 | 1 | 0 | 0 | 4 maximum throughput |
| 1 | 0 | 0 | 0 | 8 minimum delay      |

The T3 bit sets the delay. Setting T3 to 0 equals normal delay, and setting it to 1 equals low delay.

The T2 bit sets the throughput. Setting this bit to 0 equals normal throughput, and setting it to 1 equals maximum throughput. Similarly, the T1 and T0 bits set reliability and cost, respectively. Therefore, as an example, if you want to set a packet with the following requirements:

minimum delay T3 = 1

normal throughput T2 = 0

normal reliability T1 = 0

minimum monetary cost T0 = 1

You would set the ToS to 9, which is 1001 in binary format.

Use the **route-map** (IP) global configuration command with the **match** and **set** (route-map) configuration commands to define the conditions for redistributing routes from one routing protocol into another, or for policy routing. Each **route-map** command has an associated list of **match** and **set** commands. The **match** commands specify the match criteria—the conditions under which redistribution or policy routing is allowed for the current route-map command. The **set** commands specify the set actions—the particular redistribution or policy routing actions to perform if the criteria enforced by the match commands are met. The **no route-map** command deletes the route map.

The **set** (route-map) commands specify the redistribution set actions to be performed when all of the match criteria of a route map are met.

### Examples

The following example sets the IP ToS bits to 8 (minimum delay as shown in [Table 15](#)) for packets that pass the route-map match:

```
interface serial 0
 ip policy route-map texas
!
route-map texas
 match length 68 128
 set ip tos 8
!
```

### Related Commands

| Command                    | Description                                                                                                         |
|----------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>ip policy route-map</b> | Identifies a route map to use for policy routing on an interface.                                                   |
| <b>route-map (IP)</b>      | Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing. |

# set network-clocks

This command causes the router to reselect a network clock; the router selects a new clock based on clock priority.

**set network-clocks [force-reselect | next-select]**

## Syntax Description

|                       |                                                               |
|-----------------------|---------------------------------------------------------------|
| <b>force-reselect</b> | Forces the router to select a new network clock.              |
| <b>next-select</b>    | Forces the router to select the next available network clock. |

## Command Modes

Privileged EXEC

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(19)MR2 | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Examples

The following example shows how to use the set network-clocks force-reselect command:

```
Router# set network-clocks force-reselect
```

## Related Commands

| Command                    | Description                                                     |
|----------------------------|-----------------------------------------------------------------|
| <b>show network-clocks</b> | Displays information about all clocks configured on the router. |

# set precedence

To set the precedence value in the packet header, use the **set precedence** command in policy-map class configuration mode. To remove the precedence value, use the **no** form of this command.

**set precedence** {precedence-value}

**no set precedence** {precedence-value}

|                           |                         |                                                                         |
|---------------------------|-------------------------|-------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>precedence-value</i> | A number from 0 to 7 that sets the precedence bit in the packet header. |
|---------------------------|-------------------------|-------------------------------------------------------------------------|

|                        |          |
|------------------------|----------|
| <b>Command Default</b> | Disabled |
|------------------------|----------|

|                      |                                |
|----------------------|--------------------------------|
| <b>Command Modes</b> | Policy-map class configuration |
|----------------------|--------------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                           |
|------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
|                        | 12.2(13)T      | This command was introduced. This command replaces the <b>set ip precedence</b> command.                                                      |
|                        | 12.0(28)S      | Support for this command in IPv6 was added in Cisco IOS Release 12.0(28)S on the Cisco 12000 series Internet routers.                         |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                               |
|                        | 12.2(31)SB     | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router.                               |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR. This release does not support the <i>from-field</i> and <b>table</b> options.  |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not support the <i>from-field</i> and <b>table</b> options. |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | <p><b>Command Compatibility</b></p> <p>If a router is loaded with an image from this version (that is, Cisco IOS Release 12.2(13)T) that contained an old configuration, the <b>set ip precedence</b> command is still recognized. However, the <b>set precedence</b> command is used in place of the <b>set ip precedence</b> command.</p> <p>The <b>set precedence</b> command cannot be used with the <b>set dscp</b> command to mark the <i>same</i> packet. The two values, DSCP and precedence, are mutually exclusive. A packet can be one value or the other, but not both.</p> |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Bit Settings

Once the precedence bits are set, other quality of service (QoS) features such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

### Precedence Value

The network gives priority (or some type of expedited handling) to marked traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the specified precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during times of congestion.

The **set precedence** command cannot be used with the **set dscp** command to mark the *same* packet. The two values, differentiated services code point (DSCP) and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

### Using This Command with the Enhanced Packet Marking Feature

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the “from-field” packet-marking category to be used for mapping and setting the precedence value. The “from-field” packet-marking categories are as follows:

- CoS
- QoS group

If you specify a “from-field” category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action is to copy the value associated with the “from-field” category as the precedence value. For instance, if you configure the **set precedence cos** command, the CoS value is copied and used as the precedence value.

You can do the same for the QoS group-marking category. That is, you can configure the **set precedence qos-group** command, and the QoS group value is copied and used as the precedence value.

The valid value range for the precedence value is a number from 0 to 7. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set precedence qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 6), the packet-marking value is copied and the packets are marked.
- If QoS group value exceeds the precedence range (for example, 10), the packet-marking value is not copied, and the packet is not marked. No action is taken.

### Setting Precedence Values for IPv4 Packets Only

To set the precedence values for IPv4 packets only, use a command involving the **ip** keyword like the **match ip precedence** or **match ip dscp** command or include the **match protocol ip** command along with the others in the class map. Without the additional **ip** keyword, the class-map may match both IPv6 and IPv4 packets (depending on the other match criteria) and the **set precedence** or **set dscp** command may act upon both types of packets.

### Examples

The following example shows how to use the set precedence command.

```
Router(config)# policy-map policy-cos
Router(config-pmap)# class class-default
Router(config-pmap-c)# set precedence 4
Router(config-pmap-c)# end
```



The **set precedence** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface or to an ATM virtual circuit. For information on attaching a service policy to an interface, refer to the “Modular Quality of Service Command-Line Interface Overview” chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

| Related Commands | Command                          | Description                                                                                                                                                                                   |
|------------------|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>match dscp</b>                | Identifies a specific IP DSCP value as a match criterion.                                                                                                                                     |
|                  | <b>match precedence</b>          | Identifies IP precedence values as match criteria.                                                                                                                                            |
|                  | <b>match protocol</b>            | Configures the match criteria for a class map on the basis of the specified protocol.                                                                                                         |
|                  | <b>policy-map</b>                | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                                  |
|                  | <b>service-policy</b>            | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.                                                   |
|                  | <b>set cos</b>                   | Sets the Layer 2 CoS value of an outgoing packet.                                                                                                                                             |
|                  | <b>set dscp</b>                  | Marks a packet by setting the Layer 3 DSCP value in the ToS byte.                                                                                                                             |
|                  | <b>set qos-group</b>             | Sets a group ID that can be used later to classify packets.                                                                                                                                   |
|                  | <b>show policy-map</b>           | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.                                                                     |
|                  | <b>show policy-map interface</b> | Displays the configuration for all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |
|                  | <b>show table-map</b>            | Displays the configuration of a specified table map or all table maps.                                                                                                                        |
|                  | <b>table-map (value mapping)</b> | Creates and configures a mapping table for mapping and converting one packet-marking value to another.                                                                                        |

# set qos-group

To set a quality of service (QoS) group identifier (ID) that can be used later to classify packets, use the **set qos-group** command in policy-map class configuration mode. To remove the group ID, use the **no** form of this command.

**set qos-group** {*group-id*}

**no set qos-group** {*group-id*}

|                           |                                                            |                                                                                                                                                                                                                                                            |
|---------------------------|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>group-id</i> Group ID number in the range from 0 to 99. |                                                                                                                                                                                                                                                            |
| <b>Command Default</b>    | No group ID is specified.                                  |                                                                                                                                                                                                                                                            |
| <b>Command Modes</b>      | Policy-map class configuration (config-pmap-c)             |                                                                                                                                                                                                                                                            |
| <b>Command History</b>    | <b>Release</b>                                             | <b>Modification</b>                                                                                                                                                                                                                                        |
|                           | 11.1CC                                                     | This command was introduced.                                                                                                                                                                                                                               |
|                           | 12.0(5)XE                                                  | This command was integrated into Cisco IOS Release 12.0(5)XE.                                                                                                                                                                                              |
|                           | 12.0(17)SL                                                 | This command was introduced on the Cisco 10000 series router.                                                                                                                                                                                              |
|                           | 12.2(13)T                                                  | This command can now be used with the <b>random-detect discard-class-based</b> command, and this command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values. |
|                           | 12.2(18)SXE                                                | This command was integrated into Cisco IOS 12.2(18)SXE, and the <b>cos</b> keyword was added.                                                                                                                                                              |
|                           | 12.2(31)SB                                                 | This command was integrated into Cisco IOS Release 12.2(31)SB.                                                                                                                                                                                             |
|                           | Cisco IOS XE Release 2.1                                   | This command was implemented on Cisco ASR 1000 series routers.                                                                                                                                                                                             |
|                           | 12.4(20)MR                                                 | This command was integrated into Cisco IOS Release 12.4(20)MR. This release does not support the <i>from-field</i> and <b>table options</b> .                                                                                                              |
|                           | 12.2(33)MRA                                                | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not support the <i>from-field</i> and <b>table options</b> .                                                                                                             |

**Usage Guidelines**

The **set qos-group** command allows you to associate a group ID with a packet. The group ID can be used later to classify packets into QoS groups based as prefix, autonomous system, and community string.

A QoS group and discard class are required when the input per-hop behavior (PHB) marking is used for classifying packets on the output interface.

### Using This Command with the Enhanced Packet Marking Feature

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the “from-field” packet-marking category to be used for mapping and setting the precedence value.

If you specify a “from-field” category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action is to copy the value associated with the “from-field” category as the precedence value. For instance, if you enter **set qos-group precedence**, the precedence value is copied and used as the QoS group value.

A packet is marked with a QoS group value only while it is being processed within the router. The QoS group value is not included in the packet’s header when the packet is transmitted over the output interface. However, the QoS group value can be used to set the value of a Layer 2 or Layer 3 field that is included as part of the packet’s headers (such as the MPLS EXP, CoS, and DSCP fields).



#### Note

The **set qos-group cos** and **set qos-group precedence** commands are equivalent to the **mls qos trust cos** and **mls qos trust prec** commands.



#### Tip

The **set qos-group** command cannot be applied until you create a service policy in policy-map configuration mode and then attach the service policy to an interface or ATM virtual circuit (VC). For information on attaching a service policy, refer to the “Modular Quality of Service Command-Line Interface Overview” chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

### Examples

The following example shows how to set the QoS group to 1 for all packets that match the class map called class 1. These packets are then rate limited on the basis of the QoS group ID.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set qos-group 1
Router(config-pmap-c)# end
```

The following example shows how to set the QoS group value based on the packet’s original 802.1P CoS value:

```
Router(config)# policy map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set qos-group cos
Router(config-pmap-c)# end
```

### Enhanced Packet Marking Example

The following example shows how to set the QoS group value based on the values defined in a table map called table-map1. This table map is configured in a policy map called policy1. Policy map policy1 converts and propagates the QoS value according to the values defined in table-map1.

In this example, the QoS group value is set according to the precedence value defined in table-map1.

```
Router(config)# policy map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set qos-group precedence table table-map1
Router(config-pmap-c)# end
```

| Related Commands | Command                          | Description                                                                                                                                                                                  |
|------------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>match input vlan</b>          | Configures a class map to match incoming packets that have a specific VLAN ID.                                                                                                               |
|                  | <b>match qos-group</b>           | Identifies a specified QoS group value as a match criterion.                                                                                                                                 |
|                  | <b>mls qos trust</b>             | Sets the trusted state of an interface to determine which incoming QoS field on a packet, if any, should be preserved.                                                                       |
|                  | <b>policy-map</b>                | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                                 |
|                  | <b>service-policy</b>            | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.                                                  |
|                  | <b>show policy-map</b>           | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.                                                                    |
|                  | <b>show policy-map interface</b> | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# shape

To specify average or peak rate traffic shaping, use the **shape** command in class-map configuration mode. To remove traffic shaping, use the **no** form of this command.

**shape {average | peak} cir [bc] [be]**

**no shape {average | peak} cir [bc] [be]**

|                           |                |                                                                                                                                                                                                                                    |
|---------------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>average</b> | Specifies average rate shaping.                                                                                                                                                                                                    |
|                           | <b>peak</b>    | Specifies peak rate shaping.                                                                                                                                                                                                       |
|                           | <i>cir</i>     | Specifies the committed information rate (CIR), in bits per second (bps).<br>For a committed (average) burst rate, valid values are 30,000–10,000,000,000. For an excess (peak) burst rate, valid values are 8,000–10,000,000,000. |
|                           | <i>bc</i>      | (Optional) Specifies the Committed Burst size, in bits.                                                                                                                                                                            |
|                           | <i>be</i>      | (Optional) Specifies the Excess Burst size, in bits.                                                                                                                                                                               |
|                           |                |                                                                                                                                                                                                                                    |

**Command Default** Average or peak rate traffic shaping is not specified.

**Command Modes** Class-map configuration

|                        |                |                                                                                                                                                                                   |
|------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                                                               |
|                        | 12.1(2)T       | This command was introduced.                                                                                                                                                      |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                        | 12.2SX         | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

**Usage Guidelines** Traffic shaping limits the rate of transmission of data. In addition to using a specifically configured transmission rate, you can use Generic Traffic Shaping (GTS) to specify a derived transmission rate based on the level of congestion.

You can specify two types of traffic shaping; average rate shaping and peak rate shaping. Average rate shaping limits the transmission rate to the CIR. Using the CIR ensures that the average amount of traffic being sent conforms to the rate expected by the network.

Peak rate shaping configures the router to send more traffic than the CIR. To determine the peak rate, the router uses the following formula:

$$\text{peak rate} = \text{CIR}(1 + \text{Be} / \text{Bc})$$

where:

- Be is the Excess Burst size.
- Bc is the Committed Burst size.

Peak rate shaping allows the router to burst higher than average rate shaping. However, using peak rate shaping, the traffic sent above the CIR (the delta) could be dropped if the network becomes congested.

If your network has additional bandwidth available (over the provisioned CIR) and the application or class can tolerate occasional packet loss, that extra bandwidth can be exploited through the use of peak rate shaping. However, there may be occasional packet drops when network congestion occurs. If the traffic being sent to the network must strictly conform to the configured network provisioned CIR, then you should use average traffic shaping.

## Examples

The following example sets the uses average rate shaping to ensure a bandwidth of 256 kbps:

```
shape average 256000
```

The following example uses peak rate shaping to ensure a bandwidth of 300 kbps but allow throughput up to 512 kbps if enough bandwidth is available on the interface:

```
bandwidth 300
shape peak 512000
```

## Related Commands

| Command                   | Description                                                                                                                                                                   |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bandwidth</b>          | Specifies or modifies the bandwidth allocated for a class belonging to a policy map.                                                                                          |
| <b>class (policy-map)</b> | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |
| <b>policy-map</b>         | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                  |
| <b>service-policy</b>     | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.                                   |
| <b>shape max-buffers</b>  | Specifies the maximum number of buffers allowed on shaping queues.                                                                                                            |

# shape (percent)

To specify average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface, use the **shape** command in policy-map class configuration mode. To remove traffic shaping, use the **no** form of this command.

**shape { average | peak } percent *percentage* [sustained-burst-in-msec **ms**] [be *excess-burst-in-msec ms*] [bc *committed-burst-in-msec ms*]**

**no shape { average | peak } percent *percentage* [sustained-burst-in-msec **ms**] [be *excess-burst-in-msec ms*] [bc *committed-burst-in-msec ms*]**

| Syntax Description             |  |                                                                                                                             |
|--------------------------------|--|-----------------------------------------------------------------------------------------------------------------------------|
| <b>average</b>                 |  | Specifies average rate traffic shaping.                                                                                     |
| <b>peak</b>                    |  | Specifies peak rate traffic shaping.                                                                                        |
| <b>percent</b>                 |  | Specifies that a percent of bandwidth is used for either the average rate traffic shaping or peak rate traffic shaping.     |
| <i>percentage</i>              |  | Specifies the bandwidth percentage. Valid range is a number from 1 to 100.                                                  |
| <i>sustained-burst-in-msec</i> |  | (Optional) Sustained burst size used by the first token bucket for policing traffic. Valid range is a number from 4 to 200. |
| <b>ms</b>                      |  | (Optional) Indicates that the burst value is specified in milliseconds (ms).                                                |
| <b>be</b>                      |  | (Optional) Excess burst (be) size used by the second token bucket for policing traffic.                                     |
| <i>excess-burst-in-msec</i>    |  | (Optional) Specifies the be size in milliseconds. Valid range is a number from 0 to 200.                                    |
| <b>bc</b>                      |  | (Optional) Committed burst (bc) size used by the first token bucket for policing traffic.                                   |
| <i>committed-burst-in-msec</i> |  | (Optional) Specifies the bc value in milliseconds. Valid range is a number from 1 to 2000.                                  |

**Command Default** The default bc and be is 4 ms.

**Command Modes** Policy-map class configuration (config-pmap-c)

| Command History | Release     | Modification                                                                     |
|-----------------|-------------|----------------------------------------------------------------------------------|
|                 | 12.1(2)T    | This command was introduced.                                                     |
|                 | 12.2(13)T   | This command was modified for the Percentage-Based Policing and Shaping feature. |
|                 | 12.0(28)S   | The command was integrated into Cisco IOS Release 12.0(28)S.                     |
|                 | 12.2(18)SXE | The command was integrated into Cisco IOS Release 12.2(18)SXE.                   |
|                 | 12.2(28)SB  | The command was integrated into Cisco IOS Release 12.2(28)SB.                    |

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

### Committed Information Rate

This command calculates the committed information rate (CIR) on the basis of a percentage of the available bandwidth on the interface. Once a policy map is attached to the interface, the equivalent CIR value in bits per second (bps) is calculated on the basis of the interface bandwidth and the percent value entered with this command. The **show policy-map interface** command can then be used to verify the CIR bps value calculated.

The calculated CIR bps rate must be in the range of 8000 and 154,400,000 bps. If the rate is less than 8000 bps, the associated policy map cannot be attached to the interface. If the interface bandwidth changes (for example, more is added), the CIR bps values are recalculated on the basis of the revised amount of bandwidth. If the CIR percentage is changed after the policy map is attached to the interface, the bps value of the CIR is recalculated.

### Conform Burst and Peak Burst Sizes in Milliseconds

This command also allows you to specify the values for the conform burst size and the peak burst size in milliseconds. If you want bandwidth to be calculated as a percentage, the conform burst size and the peak burst size must be specified in milliseconds (ms).

The traffic shape converge rate depends on the traffic pattern and the time slice (Tc) parameter, which is directly affected by the bc that you configured. The Tc and the average rate configured are used to calculate bits per interval sustained. Therefore, to ensure that the shape rate is enforced, use a bc that results in a Tc greater than 10 ms.

### How Bandwidth Is Calculated

The **shape (percent)** command is often used in conjunction with the **bandwidth** and **priority** commands. The **bandwidth** and **priority** commands can be used to calculate the total amount of bandwidth available on an entity (for example, a physical interface). When the **bandwidth** and **priority** commands calculate the total amount of bandwidth available on an entity, the following guidelines are invoked:

- If the entity is a physical interface, the total bandwidth is the bandwidth on the physical interface.
- If the entity is a shaped ATM permanent virtual circuit (PVC), the total bandwidth is calculated as follows:
  - For a variable bit rate (VBR) virtual circuit (VC), the sustained cell rate (SCR) is used in the calculation.
  - For an available bit rate (ABR) VC, the minimum cell rate (MCR) is used in the calculation.

For more information on bandwidth allocation, see the “Congestion Management Overview” chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

## Examples

The following example configures traffic shaping using an average shaping rate on the basis of a percentage of bandwidth. In this example, 25 percent of the bandwidth has been specified. Additionally, an optional be value and bc value (100 ms and 400 ms, respectively) have been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
```



```
Router(config-pmap)# class-map class1
Router(config-pmap-c)# shape average percent 25 20 ms be 100 ms bc 400 ms
Router(config-pmap-c)# end
```

After the policy map and class maps are configured, the policy map is attached to interface as shown in the following example.

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/0
Router(config-if)# service-policy input policy1
Router(config-if)# end
```

#### Related Commands

| Command                          | Description                                                                                                                                                                  |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bandwidth</b>                 | Specifies or modifies the bandwidth allocated for a class belonging to a policy map.                                                                                         |
| <b>class (policy-map)</b>        | Specifies the name of the class whose policy you want to create or change and the default class (commonly known as the class-default class) before you configure its policy. |
| <b>police (percent)</b>          | Configures traffic policing on the basis of a percentage of bandwidth available on an interface.                                                                             |
| <b>policy-map</b>                | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                 |
| <b>priority</b>                  | Gives priority to a class of traffic belonging to a policy map.                                                                                                              |
| <b>service-policy</b>            | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.                                  |
| <b>shape max-buffers</b>         | Specifies the maximum number of buffers allowed on shaping queues.                                                                                                           |
| <b>show policy-map interface</b> | Displays the statistics and the configurations of the input and output policies that are attached to an interface.                                                           |

## shape (policy-map class)

To shape traffic to the indicated bit rate according to the algorithm specified, or to enable ATM overhead accounting, use the **shape** command in policy-map class configuration mode. To remove shaping and leave the traffic unshaped, use the **no** form of this command.

**shape** [**average** | **peak**] *mean-rate* [*burst-size*] [*excess-burst-size*]

**no shape** [**average** | **peak**]

| Syntax Description |                          |                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <b>average</b>           | (Optional) Committed Burst (Bc) is the maximum number of bits sent out in each interval.                                                                                                                                                                                                                                                                                                                                                    |
|                    | <b>peak</b>              | (Optional) Bc + Excess Burst (Be) is the maximum number of bits sent out in each interval.                                                                                                                                                                                                                                                                                                                                                  |
|                    | <i>mean-rate</i>         | (Optional) Bit rate used to shape the traffic, in bits per second (also referred to as CIR). When this command is used with backward explicit congestion notification (BECN) approximation, the bit rate is the upper bound of the range of bit rates that is permitted.<br><br>For a committed (average) burst rate, valid values are 30,000 to 10,000,000,000. For an excess (peak) burst rate, valid values are 8,000 to 10,000,000,000. |
|                    | <i>burst-size</i>        | (Optional) The number of bits in a measurement interval (Bc).                                                                                                                                                                                                                                                                                                                                                                               |
|                    | <i>excess-burst-size</i> | (Optional) The acceptable number of bits permitted to go over the Be.                                                                                                                                                                                                                                                                                                                                                                       |

| Command Default | When the excess burst size (Be) is not configured, the default Be value is equal to the committed burst size (Bc). For more information about burst size defaults, see the “Usage Guidelines” section.<br><br>Traffic shaping overhead accounting for ATM is disabled. |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| Command Modes | Policy-map class configuration (config-pmap-c) |
|---------------|------------------------------------------------|
|---------------|------------------------------------------------|

| Command History | Release     | Modification                                                                                                                 |
|-----------------|-------------|------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.0(5)XE   | This command was introduced.                                                                                                 |
|                 | 12.1(5)T    | This command was integrated into Cisco IOS Release 12.1(5)T.                                                                 |
|                 | 12.0(17)SL  | This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on the PRE1 for the Cisco 10000 series router. |
|                 | 12.2(16)BX  | This command was integrated into Cisco IOS Release 12.2(16)BX and implemented on the PRE2 for the Cisco 10000 series router. |
|                 | 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                               |
|                 | 12.2(31)SB2 | This command was enhanced for ATM overhead accounting and implemented on the Cisco 10000 series router for the PRE3.         |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                              |

| Release                  | Modification                                                                                                                                                                      |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2SX                   | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(31)SB6              | This command was enhanced to specify an offset size when calculating ATM overhead and implemented on the Cisco 10000 series router for the PRE3.                                  |
| 12.2(33)SRC              | Support for the Cisco 7600 series router was added.                                                                                                                               |
| 12.2(33)SB               | Support for the Cisco 7300 series router was added.                                                                                                                               |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers                                                                                                                     |
| 12.4(20)MR               | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
| 12.2(33)MRA              | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

### Usage Guidelines

The measurement interval is the committed burst size (Bc) divided by committed information rate (CIR). Bc cannot be set to 0. If the measurement interval is too large (greater than 128 milliseconds), the system subdivides it into smaller intervals.

If you do not specify the committed burst size (Bc) and the excess burst size (Be), the algorithm decides the default values for the shape entity. The algorithm uses a 4 milliseconds measurement interval, so Bc is  $CIR * (4 / 1000)$ .

Burst sizes larger than the default committed burst size (Bc) need to be explicitly specified. The larger the Bc, the longer the measurement interval. A long measurement interval may affect voice traffic latency, if applicable.

When the excess burst size (Be) is not configured, the default value is equal to the committed burst size (Bc).

### Examples

The following example configures a shape entity with a CIR of 1 Mbps and attaches the policy map called dts-interface-all-action to interface pos1/0/0:

```
policy-map dts-interface-all-action
  class class-interface-all
    shape average 1000000

interface pos1/0/0
  service-policy output dts-interface-all-action
```

### Traffic Shaping Overhead Accounting for ATM

When a parent policy has ATM overhead accounting enabled for shaping, you are not required to enable accounting at the child level using the **police** command. In the following configuration example, ATM overhead accounting is enabled for bandwidth on the gaming and class-default class of the child policy map named subscriber\_classes and on the class-default class of the parent policy map named subscriber\_line. The voip and video classes do not have ATM overhead accounting explicitly enabled. These priority classes have ATM overhead accounting implicitly enabled because the parent policy has ATM overhead accounting enabled. Notice that the features in the parent and child policies use the same encapsulation type.

```
policy-map subscriber_classes
  class voip
    priority level 1
    police 8000
```

■ **shape (policy-map class)**

```

class video
  priority level 2
  police 20
class gaming
  bandwidth remaining percent 80 account aal5 snap-rbe-dot1q
class class-default
  bandwidth remaining percent 20 account aal5 snap-rbe-dot1q
policy-map subscriber_line
class class-default
  bandwidth remaining ratio 10 account aal5 snap-rbe-dot1q
  shape average 512 account aal5 snap-rbe-dot1q
service policy subscriber_classes

```

**Related Commands**

| Command                    | Description                                                                                                                                                                                                     |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bandwidth</b>           | Specifies or modifies the bandwidth allocated for a class belonging to a policy map, and enables ATM overhead accounting.                                                                                       |
| <b>show policy-map</b>     | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. If configured, the command output includes information about ATM overhead accounting. |
| <b>show running-config</b> | Displays the current configuration of the router. If configured, the command output includes information about ATM overhead accounting.                                                                         |

# shape max-buffers

To specify the number of buffers allowed on shaping queues, use the **shape max-buffers** command in class-map configuration mode. To set the number of buffers to its default value, use the **no** form of this command.

**shape max-buffers** *number-of-buffers*

**no shape max-buffers**

## Syntax Description

|                          |                                                                                                             |
|--------------------------|-------------------------------------------------------------------------------------------------------------|
| <i>number-of-buffers</i> | Specifies the number of buffers. The minimum number of buffers is 1; the maximum number of buffers is 4096. |
|--------------------------|-------------------------------------------------------------------------------------------------------------|

## Command Default

1000 buffers are preset.

## Command Modes

Class-map configuration (config-cmap)

## Command History

| Release     | Modification                                                                                                                                                                        |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.1(2)T    | This command was introduced.                                                                                                                                                        |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                     |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.   |
| 12.4(20)T   | This command was integrated into Cisco IOS Release 12.4(20)T, but without support for hierarchical queueing framework (HQF). See the “Usage Guidelines” for additional information. |
| 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                      |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                     |

## Usage Guidelines

You can specify the maximum number of buffers allowed on shaping queues for each class configured to use Generic Traffic Shaping (GTS).

You configure this command under a class in a policy map. However, the **shape max-buffers** command is not supported for HQF in Cisco IOS Release 12.4(20)T. Use the **queue-limit** command, which provides similar functionality.

## Examples

The following example configures shaping and sets the maximum buffer limit to 100:

```
shape average 350000
shape max-buffers 100
```

| Related Commands | Command                   | Description                                                                                                                                                                   |
|------------------|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>bandwidth</b>          | Specifies or modifies the bandwidth allocated for a class belonging to a policy map.                                                                                          |
|                  | <b>class (policy-map)</b> | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |
|                  | <b>policy-map</b>         | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                  |
|                  | <b>queue-limit</b>        | Specifies or modifies the maximum number of packets a queue can hold for a class policy configured in a policy map.                                                           |
|                  | <b>service-policy</b>     | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.                                   |
|                  | <b>shape</b>              | Specifies average or peak rate traffic shaping.                                                                                                                               |

# show adjacency

To display information about the Cisco Express Forwarding adjacency table or the hardware Layer 3-switching adjacency table, use the **show adjacency** command in user EXEC or privileged EXEC mode.

**show adjacency** [*ip-address*] [*interface-type interface-number* | **null** *number* | **port-channel** *number* | **sysclock** *number* | **vlan** *number* | *ipv6-address* | **fcpa** *number* | **serial** *number*] [**connectionid** *number*] [**link** {**ipv4** | **ipv6** | **mpls**}] [**detail** | **encapsulation**]

**show adjacency summary** [*interface-type interface-number*]

## Syntax Description

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ip-address</i>                                       | (Optional) An IP address.                                                                                                                                                                                                                                                                                                                                                        |
| <i>interface-type</i><br><i>interface-number</i>        | (Optional) Interface type and number. Valid values for the <i>interface-type</i> argument are <b>atm</b> , <b>async</b> , <b>auto-template</b> , <b>ctunnel</b> , <b>dialer</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>group-async</b> , <b>loopback</b> , <b>mfr</b> , <b>multilink</b> , <b>tunnel</b> , <b>vif</b> , <b>virtual-template</b> , and <b>vlan</b> . |
| <b>null</b> <i>number</i>                               | (Optional) Specifies the null interface. The valid value is <b>0</b> .                                                                                                                                                                                                                                                                                                           |
| <b>vlan</b> <i>number</i>                               | (Optional) Specifies the VLAN; valid values are 1 to 4094.                                                                                                                                                                                                                                                                                                                       |
| <b>serial</b> <i>number</i>                             | (Optional) Specifies the serial interface number; valid values are 1 to 6.                                                                                                                                                                                                                                                                                                       |
| <b>connectionid</b> <i>number</i>                       | (Optional) Specifies the client connection identification number.                                                                                                                                                                                                                                                                                                                |
| <b>link</b> { <b>ipv4</b>   <b>ipv6</b>   <b>mpls</b> } | (Optional) Specifies the link type (IPv4, IPv6, or Multiprotocol Label Switching (MPLS) traffic) of the adjacency.                                                                                                                                                                                                                                                               |
| <b>detail</b>                                           | (Optional) Displays the protocol detail and timer information.                                                                                                                                                                                                                                                                                                                   |
| <b>summary</b>                                          | (Optional) Displays a summary of Cisco Express Forwarding adjacency information.                                                                                                                                                                                                                                                                                                 |

## Command Modes

User EXEC (>)  
Privileged EXEC (#)

## Command History

| Release    | Modification                                                                                                                                                                                                        |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.2GS     | This command was introduced.                                                                                                                                                                                        |
| 11.1CC     | Multiple platform support was added.                                                                                                                                                                                |
| 12.0(7)XE  | Support was added for the Cisco 7600 series routers.                                                                                                                                                                |
| 12.1(1)E   | Support was added for the Cisco 7600 series routers.                                                                                                                                                                |
| 12.1(3a)E3 | The number of valid values for <b>port-channel</b> <i>number</i> changed.                                                                                                                                           |
| 12.1(5c)EX | This command was modified to include Layer 3 information.                                                                                                                                                           |
| 12.1(11b)E | The <b>atm</b> , <b>ge-wan</b> , and <b>pos</b> keywords were added.                                                                                                                                                |
| 12.2(8)T   | The <b>detail</b> keyword output was modified to show the epoch value for each entry of the adjacency table.<br><br>The <b>summary</b> keyword output was modified to show the table epoch for the adjacency table. |
| 12.2(14)SX | Support for this command was added for the Supervisor Engine 720.                                                                                                                                                   |

| Release      | Modification                                                                                                                                                                     |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.                                                                              |
| 12.2(25)S    | This command was integrated into Cisco IOS Release 12.2(25)S. The <b>link ipv4</b> , <b>link ipv6</b> , and <b>link mpls</b> keywords and the <i>prefix</i> argument were added. |
| 12.2(28)SB   | Support for IPv6 was added for the Cisco 10000 series routers.                                                                                                                   |
| 12.2(33)SRA  | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                  |
| 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.                                                                                                                  |
| 12.4(20)T    | This command was integrated into Cisco IOS Release 12.4(20)T.                                                                                                                    |
| 12.4(20)MR   | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                   |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                  |

### Usage Guidelines

The **show adjacency** command is used to verify that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct.

For line cards, you must specify the line card if\_number (interface number). Use the **show cef interface** command to obtain line card if\_numbers.

You can use any combination of the *ip-address*, *interface-type*, and *other* keywords and arguments (in any order) as a filter to display a specific subset of adjacencies.

The following information may be displayed by the **show adjacency** commands:

- Protocol
- Interface
- Type of routing protocol that is configured on the interface
- Type of routed protocol traffic using this adjacency
- Next hop address
- Method of adjacency that was learned
- Adjacency source (for example, Address Resolution Protocol (ARP) or ATM Map)
- Encapsulation prepended to packet switched through this adjacency
- Chain of output chain elements applied to packets after an adjacency
- Packet and byte counts
- High availability (HA) epoch and summary event epoch
- MAC address of the adjacent router
- Time left before the adjacency rolls out of the adjacency table. After the adjacency rolls out, a packet must use the same next hop to the destination.

### Examples

The following example shows how to display a summary of adjacency information:

```
Router# show adjacency summary
```

```
Adjacency table has 7 adjacencies:
  each adjacency consumes 368 bytes (4 bytes platform extension)
  6 complete adjacencies
  1 incomplete adjacency
```



```

4 adjacencies of linktype IP
  4 complete adjacencies of linktype IP
  0 incomplete adjacencies of linktype IP
  0 adjacencies with fixups of linktype IP
  2 adjacencies with IP redirect of linktype IP
3 adjacencies of linktype IPV6
  2 complete adjacencies of linktype IPV6
  1 incomplete adjacency of linktype IPV6

Adjacency database high availability:
  Database epoch: 8 (7 entries at this epoch)

Adjacency manager summary event processing:
  Summary events epoch is 52
  Summary events queue contains 0 events (high water mark 113 events)
  Summary events queue can contain 49151 events
  Adj last sourced field refreshed every 16384 summary events
RP adjacency component enabled

```

## Related Commands

| Command                   | Description                                                                |
|---------------------------|----------------------------------------------------------------------------|
| <b>clear adjacency</b>    | Clears the Cisco Express Forwarding adjacency table.                       |
| <b>clear arp-cache</b>    | Deletes all dynamic entries from the ARP cache.                            |
| <b>show adjacency</b>     | Enables the display of information about the adjacency database.           |
| <b>show cef interface</b> | Displays detailed Cisco Express Forwarding information for all interfaces. |

# show atm cell-packing

To display cell packing information for the Layer 2 attachment circuits (ACs) configured on your system, use the **show atm cell-packing** command in privileged EXEC mode.

**show atm cell-packing**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Examples** The following example shows output from the **show atm cell-packing** command:

```
Router# show atm cell-packing
```

|                |          | avg # |           | avg #      |           |      |
|----------------|----------|-------|-----------|------------|-----------|------|
| Circuit        |          | local | cells/pkt | negotiated | cells/pkt | MCPT |
| Type           |          | MNCP  | rcvd      | MNCP       | sent      | (us) |
| ATM0/2/0/1.200 | vc 1/200 | 1     | 0         | 1          | 0         | 50   |
| ATM0/2/0/1.300 | vc 1/300 | 1     | 0         | 1          | 0         | 50   |

| Related Commands | Command                 | Description                                               |
|------------------|-------------------------|-----------------------------------------------------------|
|                  | <b>cell-packing</b>     | Packs multiple ATM cells into each MPLS or L2TPv3 packet. |
|                  | <b>atm cell-packing</b> | Packs multiple ATM cells into each MPLS or L2TPv3 packet. |

# show cem circuit

To display a summary of CEM circuits, use the **show cem circuit** command in privileged EXEC mode.

**show cem circuit** [*cem-id*]

| Syntax Description | <i>cem-id</i> | (Optional) Identifies the circuit configured with the <b>cem-group</b> command. |
|--------------------|---------------|---------------------------------------------------------------------------------|
|--------------------|---------------|---------------------------------------------------------------------------------|

| Command Modes | Privileged EXEC |
|---------------|-----------------|
|---------------|-----------------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(12)MR2 | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Examples

The following examples show the output generated by this command;

```
Router# show cem circuit
CEM Int.      ID   Ctrlr   Admin   Circuit   AC
-----
CEM0/0        0   UP      UP      Enabled   UP
CEM0/1        1   UP      UP      Enabled   UP
CEM0/2        2   UP      UP      Enabled   UP
CEM0/3        3   UP      UP      Enabled   UP
CEM0/4        4   UP      UP      Enabled   UP
CEM0/5        5   UP      UP      Enabled   UP

Router# show cem circuit 5

CEM0/5, ID: 5, Line: UP, Admin: UP, Ckt: Enabled
Controller state: up
Idle Pattern: 0xFF, Idle cas: 0x8
Dejitter: 4, Sample Rate: 1, Payload Size: 192
Framing: Framed, (DS0 channels: 1-24)
CEM Defects Set
None

Signalling: No CAS
RTP: No RTP

Ingress Pkts:   527521938           Dropped:           0
Egress Pkts:   527521938           Dropped:           0

CEM Counter Details
Input Errors:   0                   Output Errors:      0
Pkts Missing:   0                   Pkts Reordered:     0
Misorder Drops: 0                   JitterBuf Underrun: 0
Error Sec:      0                   Severly Errored Sec: 0
Unavailable Sec: 0                   Failure Counts:      0
Pkts Malformed: 0
```

| Related Commands | Command                  | Description                                                     |
|------------------|--------------------------|-----------------------------------------------------------------|
|                  | show cem circuit detail  | Displays detailed information about all CEM circuits.           |
|                  | show cem platform        | Displays platform-specific error counters for all CEM circuits. |
|                  | show cem platform errors | Displays platform-specific error counters for all CEM circuits. |

# show cem platform

To display platform-specific error counters for all CEM circuits, use the **show cem platform** command in privileged EXEC mode.

**show cem platform** [*interface*]

|                           |                                                                                 |
|---------------------------|---------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>interface</i> (Optional) Identifies the CEM interface (for example, CEM0/1). |
|---------------------------|---------------------------------------------------------------------------------|

|                      |                 |
|----------------------|-----------------|
| <b>Command Modes</b> | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(12)MR2 | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Examples

The following examples show the output generated by this command:

```
Router# show cem platform
CEM0/0 errors:
  net2cem_drops ===== 50/527658758
  net2cem_drops_underflow == 26
  net2cem_drops_overflow === 24
  Last cleared 6d02h
CEM0/1 errors:
  net2cem_drops ===== 50/527658759
  net2cem_drops_underflow == 25
  net2cem_drops_overflow === 25
  Last cleared 6d02h
CEM0/2 errors:
  net2cem_drops ===== 2/526990836
  net2cem_drops_overflow === 2
  Last cleared never
CEM0/3 errors:
  net2cem_drops ===== 1/526982274
  net2cem_drops_overflow === 1
  Last cleared never
CEM0/4 errors:
  net2cem_drops ===== 51/527658758
  net2cem_drops_underflow == 26
  net2cem_drops_overflow === 25
  Last cleared 6d02h
CEM0/5 errors:
  net2cem_drops ===== 48/527660498
  net2cem_drops_underflow == 24
  net2cem_drops_overflow === 24
  Last cleared 6d02h
```

```
Router# show cem platform cem0/1
CEM0/1 errors:
  net2cem_drops ===== 50/527678398
  net2cem_drops_underflow == 25
  net2cem_drops_overflow === 25
```

**show cem platform**

Last cleared 6d02h

| Related Commands | Command                         | Description                                                     |
|------------------|---------------------------------|-----------------------------------------------------------------|
|                  | <b>show cem circuit</b>         | Displays a summary of CEM circuits.                             |
|                  | <b>show cem circuit detail</b>  | Displays detailed information about all CEM circuits.           |
|                  | <b>show cem platform errors</b> | Displays platform-specific error counters for all CEM circuits. |

# show connection

To display the status of interworking connections, use the **show connection** command in privileged EXEC mode.

**show connection** [**all** | *element* | **id** *ID* | **name** *name* | **port** *port*]

## Syntax Description

|                         |                                                                                                                                                                 |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>all</b>              | (Optional) Displays information about all interworking connections.                                                                                             |
| <i>element</i>          | (Optional) Displays information about the specified connection element.                                                                                         |
| <b>id</b> <i>ID</i>     | (Optional) Displays information about the specified connection identifier.                                                                                      |
| <b>name</b> <i>name</i> | (Optional) Displays information about the specified connection name.                                                                                            |
| <b>port</b> <i>port</i> | (Optional) Displays information about all connections on an interface. (In Cisco IOS Release 12.0S, only ATM, serial, and Fast Ethernet connections are shown.) |

## Command Modes

Privileged EXEC

## Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.1(2)T    | This command was introduced as <b>show connect</b> (FR-ATM).                                                                                                                      |
| 12.0(27)S   | This command was integrated into Cisco IOS Release 12.0(27)S and updated to show all ATM, serial, and Fast Ethernet interworking connections.                                     |
| 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.                                                                                                                     |
| 12.4(2)T    | The command output was changed to add Segment 1 and Segment 2 fields for Segment state and channel ID.                                                                            |
| 12.0(30)S   | This command was integrated into Cisco IOS Release 12.0(30)S.                                                                                                                     |
| 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                                                                    |
| 12.4(8)     | This command was integrated into Cisco IOS Release 12.4(8).                                                                                                                       |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.4(11)T   | This command was integrated into Cisco IOS Release 12.4(11)T.                                                                                                                     |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2.                                                                                                                   |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

**Examples**

The following example shows the local interworking connections on a router:

```
Router# show connection
ID   Name                               Segment 1                Segment 2                State
=====
1    conn1                             ATM 1/0/0 AAL5 0/100     ATM 2/0/0 AAL5 0/100     UP
2    conn2                             ATM 2/0/0 AAL5 0/300     Serial0/1 16             UP
3    conn3                             ATM 2/0/0 AAL5 0/400     FA 0/0.1 10             UP
4    conn4                             ATM 1/0/0 CELL 0/500     ATM 2/0/0 CELL 0/500     UP
5    conn5                             ATM 1/0/0 CELL 100       ATM 2/0/0 CELL 100       UP
```

Table B-16 describes the significant fields shown in the display.

**Table B-16** *show connection Field Descriptions*

| Field                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ID                     | Arbitrary connection identifier assigned by the operating system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Name                   | Name of the connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Segment 1<br>Segment 2 | Information about the interworking segments, including: <ul style="list-style-type: none"> <li>Interface name and number.</li> <li>Segment state, interface name and number, and channel ID. Segment state displays nothing if the segment state is UP, “-” if the segment state is DOWN, and “***Card Removed***” if the segment state is DETACHED.</li> <li>Type of encapsulation (if any) assigned to the interface.</li> <li>Permanent virtual circuit (PVC) assigned to the ATM interface, data-link connection identifier (DLCI) assigned to the serial interface, or VLAN ID assigned to the Ethernet interface.</li> </ul> |
| State or Status        | Status of the connection, which is one of the following: INVALID, UP, ADMIN UP, ADMIN DOWN, OPER DOWN, COMING UP, NOT VERIFIED, ERR.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Related Commands**

| Command                     | Description                                    |
|-----------------------------|------------------------------------------------|
| <b>show atm pvc</b>         | Displays the status of ATM PVCs and SVCs.      |
| <b>show frame-relay pvc</b> | Displays the status of Frame Relay interfaces. |



# show controller

Use the **show controller** command to display the status of an interface.

**show controller** {ATM | Async | BITS | CEM | E1 | GigabitEthernet | J1 | SHDSL | T1 | RTM}  
*slot / port*

## Syntax Description

|                        |                                                         |
|------------------------|---------------------------------------------------------|
| <b>ATM</b>             | Displays the status of the ATM controller.              |
| <b>Async</b>           | Displays the status of the async controller.            |
| <b>BITS</b>            | Displays the status of the BITS controller.             |
| <b>CEM</b>             | Displays the status of the CEM controller.              |
| <b>E1</b>              | Displays the status of the E1 controller.               |
| <b>GigabitEthernet</b> | Displays the status of the Gigabit Ethernet controller. |
| <b>J1</b>              | Displays the status of the J1 controller.               |
| <b>SHDSL</b>           | Displays the status of the SHDSL controller.            |
| <b>T1</b>              | Displays the status of the T1 controller.               |
| <b>rtm</b>             | Displays the status of the RTM controller.              |
| <i>slot</i>            | The slot number of the interface.                       |
| <i>port</i>            | The port number of the interface.                       |

## Command Modes

Privileged EXEC

## Command History

| Release     | Modification                                                                                                         |
|-------------|----------------------------------------------------------------------------------------------------------------------|
| 12.4(19)MR2 | This command was incorporated.                                                                                       |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not provide support for DSL HWICs. |


## Examples

```
Router# show controller e1 0/2
E1 0/2 is up.
  Applique type is Channelized E1 - balanced
  No alarms detected.
  alarm-trigger is not set
  Version info Firmware: 20050421, FPGA: 13, spm_count = 0
  Daughter card FPGA version: 0x16, source: Bundled
  Framing is NO-CRC4, Line Code is HDB3, Clock Source is Line.
  CRC Threshold is 320. Reported from firmware is 320.
  VWIC relays are closed
  Link noise monitor disabled
  Data in current interval (330 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    243 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
```



### Note

The last line of the example shows 243 Slip Secs, indicating a possible clocking issue.

 show controller

| Related Commands | Command      | Description                               |
|------------------|--------------|-------------------------------------------|
|                  | show atm pvc | Displays the status of ATM PVCs and SVCs. |

# show cns config connections

To display the status of the Cisco Networking Services (CNS) event agent connection, use the **show cns config connections** command in privileged EXEC mode.

**show cns config connections**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(8)T    | This command was introduced.                                    |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** Use the **show cns config connections** command to determine whether the CNS event agent is connecting to the gateway, connected, or active, and to display the gateway used by the event agent and its IP address and port number.

**Examples** The following is sample output from the **show cns config connections** command:

```
Router# show cns config connections

The partial configuration agent is enabled.

Configuration server: 10.1.1.1
Port number:         80
Encryption:          disabled
Config id:            test1
Connection Status:    Connection not active.
```

| Related Commands | Command                            | Description                                                                                        |
|------------------|------------------------------------|----------------------------------------------------------------------------------------------------|
|                  | <b>show cns config outstanding</b> | Displays information about incremental CNS configurations that have started but not yet completed. |
|                  | <b>show cns config stats</b>       | Displays statistics about the CNS configuration agent.                                             |

# show cns config outstanding

To display information about incremental (partial) Cisco Networking Services (CNS) configurations that have started but not yet completed, use the **show cns config outstanding** command in privileged EXEC mode.

**show cns config outstanding**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification                                                                     |
|-----------------|-------------|----------------------------------------------------------------------------------|
|                 | 12.2(2)T    | This command was introduced.                                                     |
|                 | 12.2(8)T    | This command was implemented on Cisco 2600 series and Cisco 3600 series routers. |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.                   |
|                 | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI.                  |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                   |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                  |

**Usage Guidelines** Use the **show cns config outstanding** command to display information about outstanding incremental (partial) configurations that have started but not yet completed, including the following:

- Queue ID (location of configuration in the config queue)
- Identifier (group ID)
- Config ID (identity of configuration within the group)

**Examples** The following is sample output from the **show cns config outstanding** command:

```
Router# show cns config outstanding
```

```
The outstanding configuration information:
```

```
queue id    identifier    config-id
1           identifierREAD  config_idREAD
```

| Related Commands | Command                      | Description                                                     |
|------------------|------------------------------|-----------------------------------------------------------------|
|                  | <b>cns config cancel</b>     | Cancels an incremental two-phase synchronization configuration. |
|                  | <b>config-cli</b>            | Displays the status of the CNS event agent connection.          |
|                  | <b>show cns config stats</b> | Displays statistics about the CNS configuration agent.          |

# show cns config stats

To display statistics about the Cisco Networking Services (CNS) configuration agent, use the **show cns config stats** command in privileged EXEC mode.

**show cns config stats**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification                                                                     |
|-----------------|-------------|----------------------------------------------------------------------------------|
|                 | 12.2(2)T    | This command was introduced.                                                     |
|                 | 12.2(8)T    | This command was implemented on Cisco 2600 series and Cisco 3600 series routers. |
|                 | 12.3(1)     | Additional output fields were added.                                             |
|                 | 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.                    |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                  |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.                   |
|                 | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI.                  |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                   |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                  |

**Usage Guidelines** This command displays the following statistics on the CNS configuration agent:

- Number of configurations requests received
- Number of configurations completed
- Number of configurations failed
- Number of configurations pending
- Number of configurations cancelled
- Time stamp of the last configuration received
- Time stamp of the initial configuration received

---

**Examples**

The following is sample output from the **show cns config stats** command:

```
Router# show cns config stats

6 configuration requests received.
4 configurations completed.
1 configurations failed.
1 configurations pending.
0 configurations cancelled.
The time of last received configuration is *May 5 2003 10:42:15 UTC.
Initial Config received *May 5 2003 10:45:15 UTC.
```

---

**Related Commands**

| Command                            | Description                                                                                        |
|------------------------------------|----------------------------------------------------------------------------------------------------|
| <b>clear cns config stats</b>      | Clears all the statistics about the CNS configuration agent.                                       |
| <b>show cns config outstanding</b> | Displays information about incremental CNS configurations that have started but not yet completed. |

# show cns event connections

To display the status of the Cisco Networking Services (CNS) event agent connection, use the **show cns event connections** command in privileged EXEC mode.

## show cns event connections

|                           |                                            |
|---------------------------|--------------------------------------------|
| <b>Syntax Description</b> | This command has no arguments or keywords. |
|---------------------------|--------------------------------------------|

|                      |                     |
|----------------------|---------------------|
| <b>Command Modes</b> | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(8)T    | This command was introduced.                                    |
|                 | 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.   |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
|                 | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                                                                                                                                                                                                                                                    |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | Use the <b>show cns event connections</b> command to display the status of the event agent connection—such as whether it is connecting to the gateway, connected, or active—and to display the gateway used by the event agent and its IP address and port number. |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------|
| <b>Examples</b> | The following example displays the IP address and port number of the primary and backup gateways: |
|-----------------|---------------------------------------------------------------------------------------------------|

```
Router# show cns event connections
```

```
The currently configured primary event gateway:
```

```
    hostname is 10.1.1.1.
```

```
    port number is 11011.
```

```
Event-Id is Internal test1
```

```
Keepalive setting:
```

```
    none.
```

```
Connection status:
```

```
    Connection Established.
```

```
The currently configured backup event gateway:
```

```
    none.
```

```
The currently connected event gateway:
```

```
    hostname is 10.1.1.1.
```

```
    port number is 11011.
```

| Related Commands | Command                | Description                                                       |
|------------------|------------------------|-------------------------------------------------------------------|
|                  | show cns event stats   | Displays statistics about the CNS event agent connection.         |
|                  | show cns event subject | Displays a list of subjects about the CNS event agent connection. |



# show cns event stats

To display statistics about the Cisco Networking Services (CNS) event agent connection, use the **show cns event stats** command in privileged EXEC mode.

**show cns event stats**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification                                                                             |
|-----------------|-------------|------------------------------------------------------------------------------------------|
|                 | 12.2(2)T    | This command was introduced.                                                             |
|                 | 12.0(18)ST  | This command was integrated into Cisco IOS Release 12.0(18)ST.                           |
|                 | 12.0(22)S   | This command was integrated into Cisco IOS Release 12.0(22)S.                            |
|                 | 12.2(8)T    | This command was implemented on the Cisco 2600 series and the Cisco 3600 series routers. |
|                 | 12.3(1)     | Output was changed to display statistics generated since last cleared.                   |
|                 | 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.                            |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                          |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.                           |
|                 | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI.                          |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                           |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                          |

**Usage Guidelines** Use this command to display the following statistics for the CNS event agent:

- Number of events received
- Number of events sent
- Number of events not processed successfully
- Number of events in the queue
- Time stamp showing when statistics were last cleared (time stamp is router time)
- Number of events received since the statistics were cleared
- Time stamp of latest event received (time stamp is router time)
- Time stamp of latest event sent
- Number of applications using the Event Agent
- Number of subjects subscribed

**Examples**

The following example displays statistics for the CNS event agent:

```
Router# show cns event stats

0 events received.
1 events sent.
0 events not processed.
0 events in the queue.
0 events sent to other IOS applications.
Event agent stats last cleared at Apr 4 2003 00:55:25 UTC
No events received since stats cleared
The time stamp of the last received event is *Mar 30 2003 11:04:08 UTC
The time stamp of the last sent event is *Apr 11 2003 22:21:23 UTC
3 applications are using the event agent.
0 subjects subscribed.
1 subjects produced.
0 subjects replied.
```

**Related Commands**

| Command                           | Description                                                       |
|-----------------------------------|-------------------------------------------------------------------|
| <b>clear cns event stats</b>      | Clears all the statistics about the CNS event agent.              |
| <b>cns event</b>                  | Enables and configures CNS event agent services.                  |
| <b>show cns event connections</b> | Displays the status of the CNS event agent connection.            |
| <b>show cns event subject</b>     | Displays a list of subjects about the CNS event agent connection. |

# show cns event subject

To display a list of subjects about the Cisco Networking Services (CNS) event agent connection, use the **show cns event subject** command in privileged EXEC mode.

**show cns event subject** [*name*]

|                           |             |                                                                                                |
|---------------------------|-------------|------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>name</i> | (Optional) Displays a list of applications that are subscribing to this specific subject name. |
|---------------------------|-------------|------------------------------------------------------------------------------------------------|

|                      |                     |
|----------------------|---------------------|
| <b>Command Modes</b> | Privileged EXEC (#) |
|----------------------|---------------------|

| <b>Command History</b> | Release     | Modification                                                                     |
|------------------------|-------------|----------------------------------------------------------------------------------|
|                        | 12.2(2)T    | This command was introduced.                                                     |
|                        | 12.0(18)ST  | This command was integrated into Cisco IOS Release 12.0(18)ST.                   |
|                        | 12.0(22)S   | This command was integrated into Cisco IOS Release 12.0(22)S.                    |
|                        | 12.2(8)T    | This command was implemented on the Cisco 2600 series and the Cisco 3600 series. |
|                        | 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.                    |
|                        | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                  |
|                        | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.                   |
|                        | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI.                  |
|                        | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.                   |
|                        | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                  |

|                         |                                                                                                                                        |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | Use the <b>show cns event subject</b> command to display a list of subjects of the event agent that are subscribed to by applications. |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------|
| <b>Examples</b> | The following example displays the IP address and port number of the primary and backup gateways: |
|-----------------|---------------------------------------------------------------------------------------------------|

```
Router# show cns event subject
```

```
The list of subjects subscribed by applications.
cisco.cns.mibaccess:request
cisco.cns.config.load
cisco.cns.config.reboot
cisco.cns.exec.cmd
```

| <b>Related Commands</b> | Command                           | Description                                               |
|-------------------------|-----------------------------------|-----------------------------------------------------------|
|                         | <b>show cns event connections</b> | Displays the status of the CNS event agent connection.    |
|                         | <b>show cns event stats</b>       | Displays statistics about the CNS event agent connection. |

# show cns image connections

To display the status of the Cisco Networking Services (CNS) image management server HTTP connections, use the **show cns image connections** command in privileged EXEC mode.

## show cns image connections

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.3(1)     | This command was introduced.                                    |
|                 | 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
|                 | 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
|                 | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** Use the **show cns image connections** command when troubleshooting HTTP connection problems with the CNS image server. The output displays the following information:

- Number of connection attempts
- Number of connections that were never connected and those that were abruptly disconnected
- Date and time of last successful connection

**Examples** The following is sample output from the **show cns image connections** command:

```
Router# show cns image connections

CNS Image Agent: HTTP connections
Connection attempts 1
never connected:0   Abrupt disconnect:0
Last successful connection at 11:45:02.000 UTC Mon May 6 2003
```

| Related Commands | Command                         | Description                                               |
|------------------|---------------------------------|-----------------------------------------------------------|
|                  | <b>show cns image inventory</b> | Displays inventory information about the CNS image agent. |
|                  | <b>show cns image status</b>    | Displays status information about the CNS image agent.    |

# show cns image inventory

To provide a dump of Cisco Networking Services (CNS) image inventory information in extensible markup language (XML) format, use the **show cns image inventory** command in privileged EXEC mode.

## show cns image inventory

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.3(1)     | This command was introduced.                                    |
|                 | 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
|                 | 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
|                 | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** To view the XML output in a better format, paste the content into a text file and use an XML viewing tool.

**Examples** The following is sample output from the **show cns image inventory** command:

```
Router# show cns image inventory
```

```
Inventory Report
<imageInventoryReport><deviceName><imageID>Router</imageID><hostName>Router</ho
IOS (tm) C2600 Software (C2600-I-M), Experimental Version 12.3(20030414:081500)]
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 14-Apr-03 02:03 by engineer</versionString><imageFile>tftp://10.25>
```

| Related Commands | Command                           | Description                                              |
|------------------|-----------------------------------|----------------------------------------------------------|
|                  | <b>show cns image connections</b> | Displays connection information for the CNS image agent. |
|                  | <b>show cns image status</b>      | Displays status information about the CNS image agent.   |

# show cns image status

To display status information about the Cisco Networking Services (CNS) image agent, use the **show cns image status** command in privileged EXEC mode.

**show cns image status**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.3(1)     | This command was introduced.                                    |
|                 | 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
|                 | 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
|                 | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |
|                 | 12.4(20)MR  | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** Use this command to display the following status information about the CNS image agent:

- Start date and time of last upgrade
- End date and time of last upgrade
- End date and time of last successful upgrade
- End date and time of last failed upgrade
- Number of failed upgrades
- Number of successful upgrades with number of received messages and errors
- Transmit status with number of attempts, successes, and failures

**Examples** The following is sample output from the **show cns image status** command:

```
Router# show cns image status

Last upgrade started at 11:45:02.000 UTC Mon May 6 2003
Last upgrade ended at 11:56:04.000 UTC Mon May 6 2003 status SUCCESS

Last successful upgrade ended at 00:00:00.000 UTC Mon May 6 2003
Last failed upgrade ended at 00:00:00.000 UTC Wed Apr 16 2003
Number of failed upgrades: 2
Number of successful upgrades: 6
  messages received: 12
  receive errors: 5
Transmit Status
```

```
TX Attempts:4
  Successes:3      Failures 2
```

| Related Commands | Command                           | Description                                              |
|------------------|-----------------------------------|----------------------------------------------------------|
|                  | <b>show cns image connections</b> | Displays connection information for the CNS image agent. |
|                  | <b>show cns image inventory</b>   | Displays image inventory information in XML format.      |

# show ethernet cfm domain

To display information for an Ethernet connectivity fault management (CFM) domain, use the **show ethernet cfm domain** command in privileged EXEC mode.

**show ethernet cfm domain** [*domain-name* | **brief**]

## Syntax Description

|                    |                                                                                       |
|--------------------|---------------------------------------------------------------------------------------|
| <i>domain-name</i> | (Optional) String of a maximum of 154 characters.                                     |
| <b>brief</b>       | (Optional) Specifies a display of brief details about configured maintenance domains. |

## Command Default

All information about all the configured domains is displayed when the optional keywords are not used.

## Command Modes

Privileged EXEC (#)

## Command History

| Release      | Modification                                                    |
|--------------|-----------------------------------------------------------------|
| 12.2(33)SX12 | This command was introduced.                                    |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

When a domain name is not specified, information for all domains is shown.

If a domain name has more than 43 characters, a warning message is displayed notifying that the maintenance domain ID (MDID) are truncated to 43 characters in continuity check messages (CCMs) if “id <fmt> <MDID>” is not configured.

When the **brief** keyword is used, the command output shows the following summary data:

- Domain name
- Domain index
- Domain level
- Number of maintenance associations in the domain
- Archive hold time for the error and continuity check databases for the domain

## Examples

Following is sample output from a **show ethernet cfm domain** command using the **brief** keyword:

Router# **show ethernet cfm domain brief**

```

Domain Name                               Index Level Services Archive(min)
Domain_L7                                19      7         1       100
Domain_L5                                20      5         1       100
Domain_port                              18      0         1       100
Router1-cfm#

```



Table 17 describes the significant fields shown in the display.

**Table 17** *show ethernet cfm domain brief Field Descriptions*

| Field        | Description                                                                                                                                                                               |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Domain Name  | Name of the domain.                                                                                                                                                                       |
| Index        | Running counter                                                                                                                                                                           |
| Level        | Maintenance domain level.                                                                                                                                                                 |
| Services     | Number of services running.                                                                                                                                                               |
| Archive(min) | Number of the minutes that data from a missing maintenance endpoint (MEP) is kept in the continuity check database or that entries are held in the error database before they are purged. |

Following is sample output from a **show ethernet cfm domain** command when neither of the options is used:

Router# **show ethernet cfm domain**

```

Domain Name: Domain_L7
Level: 7
Total Services : 1
  Services:
    VLAN Dir CC CC-int Static-rmep Crosscheck MaxMEP MA-Name
    11  Up  Y  10s    Disabled    Disabled    100    cust_700_17

Domain Name: Domain_L5
Level: 5
Total Services : 1
  Services:
    VLAN Dir CC CC-int Static-rmep Crosscheck MaxMEP MA-Name
    9   Up  Y  10s    Disabled    Disabled    100    cust_500_15

Domain Name: Domain_port
Level: 0
Total Services : 1
  Services:
    VLAN Dir CC CC-int Static-rmep Crosscheck MaxMEP MA-Name
none Dwn Y  10s    Disabled    Disabled    100    portmep

```

Table 18 describes the significant fields shown in the display.

**Table 18** *show ethernet cfm domain Field Descriptions*

| Field          | Description                                                     |
|----------------|-----------------------------------------------------------------|
| Domain Name    | Name of the domain.                                             |
| Level          | Maintenance domain level.                                       |
| Total Services | Number of services running.                                     |
| Services       | The services currently running.                                 |
| VLAN           | Number of the VLAN.                                             |
| Dir            | Either up (toward the switch) or down (toward the LAN or wire). |

**Table 18** *show ethernet cfm domain Field Descriptions (continued)*

| Field       | Description                                                  |
|-------------|--------------------------------------------------------------|
| CC          | Continuity Check message (CCM) status (enabled or disabled). |
| CC-int      | Time between CCMs.                                           |
| Static-rmep | Status of the remote MEP.                                    |
| Crosscheck  | Status of the cross-check function.                          |
| MaxMEP      | Number of maximum MEPs allowed.                              |
| MA-Name     | Name of the maintenance association.                         |

**Related Commands**

| Command                                                       | Description                                                                                       |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>show ethernet cfm maintenance-points remote</b>            | Displays information about remote maintenance points in the continuity check database.            |
| <b>show ethernet cfm maintenance-points remote crosscheck</b> | Displays information about remote maintenance points configured statically in a cross-check list. |
| <b>show ethernet cfm maintenance-points remote detail</b>     | Displays information about a remote maintenance point in the continuity check database.           |

# show ethernet cfm errors

To display connectivity fault management (CFM) continuity check error conditions logged on a device since it was last reset or since the log was last cleared, use the **show ethernet cfm errors** command in privileged EXEC mode.



## Note

Release 12.2(33)MRA supports the Draft 1.0 version of Ethernet CFM; it does not support the IEEE 802.1ag-2007 version.

### Cisco pre-Standard CFM Draft 1 (CFM D1)

**show ethernet cfm errors** [**domain** *domain-name* | **level** *level-id*]

### CFM IEEE 802.1ag Standard (CFM IEEE)

**show ethernet cfm errors** [**configuration** | **domain-id** {*mac address* | *domain-name* | **dns** *dns-name* | **null**} [**service** {*ma-name* | *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*}] ]

## Syntax Description

|                      |                                                                                                             |
|----------------------|-------------------------------------------------------------------------------------------------------------|
| <b>domain</b>        | (Optional) Indicates that a maintenance domain is specified.                                                |
| <i>domain-name</i>   | (Optional) String of a maximum of 154 characters.                                                           |
| <b>level</b>         | (Optional) Indicates that a maintenance level is specified.                                                 |
| <i>level-id</i>      | (Optional) Integer from 0 to 7 that identifies the maintenance level.                                       |
| <b>configuration</b> | (Optional) Displays the configuration error list information; for example, port, VLAN, and error condition. |
| <b>domain-id</b>     | (Optional) Displays by domain ID.                                                                           |
| <i>mac-address</i>   | (Optional) MAC address of the maintenance domain.                                                           |
| <b>dns</b>           | (Optional) Displays a domain name service (DNS).                                                            |
| <i>dns-name</i>      | (Optional) String of a maximum of 43 characters.                                                            |
| <b>null</b>          | (Optional) Indicates there is not a domain name.                                                            |
| <b>service</b>       | (Optional) Displays a maintenance association within the domain.                                            |
| <i>ma-name</i>       | (Optional) String that identifies the maintenance association.                                              |
| <i>ma-num</i>        | (Optional) Integer that identifies the maintenance association.                                             |
| <b>vlan-id</b>       | (Optional) Displays a VLAN.                                                                                 |
| <i>vlan-id</i>       | (Optional) Integer from 1 to 4094 that identifies the VLAN.                                                 |
| <b>vpn-id</b>        | (Optional) Displays a virtual private network (VPN).                                                        |
| <i>vpn-id</i>        | (Optional) Integer from 1 to 32767 that identifies the VPN.                                                 |

## Command Default

In CFM IEEE, when no maintenance domain is specified, errors for all domains are displayed.

In CFM D1, when no maintenance domain or maintenance level is specified, errors for all domains and all levels are displayed.

## Command Modes

Privileged EXEC (#)

**Command History**

| Release      | Modification                                                     |
|--------------|------------------------------------------------------------------|
| 12.2(33)SRA  | This command was introduced.                                     |
| 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T.    |
| 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.  |
| 12.2(33)SXI2 | This command was integrated into Cisco IOS Release 12.2(33)SXI2. |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.  |

**Usage Guidelines**

Errors that are logged and that the **show ethernet cfm errors** command displays depend on the version of CFM that is running. Errors include the following:

- MEP-Down—Maintenance End Point (MEP) timed out or is advertising a 0 lifetime.
- Configuration Error—A continuity check message (CCM) is received that has an maintenance point ID (MPID) matching the local device, but the source MAC address is different.
- Forwarding Loop—A CCM is received, that has the same MPID and same MAC address as the local device.
- Cross-connected—A CCM is received and the service ID does not match the service ID configured on the device for that VLAN.
- Cross-check Missing MEP—The cross-checking delay timer has expired, and the configured remote MEP did not come up.
- Cross-check Unknown MEP—An unexpected remote MEP came up.
- Receive AIS—A MEP detects a mismerge, which is an unexpected MEP condition, or a signal fail condition resulting in peer MEPs receiving an alarm indication signal (AIS) frame.

Error conditions are kept in a log for the duration of the archive hold time configured on the maintenance domain or until the error condition is cleared, whichever occurs first.

**Examples**

The following example shows CFM IEEE sample output from a **show ethernet cfm errors** command using none of the optional keywords or arguments:

```
Router# show ethernet cfm errors
```

```
-----
MPID Domain Id          Mac Address      Type   Id   Lvl
      MAName              Reason           Age
-----
37   Domain_port        aabb.cc03.ba00   Port   none 0
      portmep           Lifetime Timer Expired 89s
401  Domain_L5          aabb.cc03.bb99   Vlan   9    5
      cust_500_15       Lifetime Timer Expired 88s
301  Domain_L7          aabb.cc03.bb99   Vlan   11   7
      cust_700_17       Lifetime Timer Expired 86s
-----
```

Table 19 describes the significant fields shown in the display.

**Table 19** *show ethernet cfm errors Field Descriptions*

| Field       | Description                                                   |
|-------------|---------------------------------------------------------------|
| MPID        | Identifier of the MEP on which the error occurred.            |
| Domain Id   | Identifier of the domain affected by the error.               |
| Mac Address | MAC address of the remote MEP on which the error occurred.    |
| Type        | Type of MEP (VLAN or port MEP)                                |
| Id          | Identifier of the VLAN on which the error occurred.           |
| Lvl         | Maintenance level at which the error occurred.                |
| MAName      | Name of the maintenance association where the error occurred. |
| Reason      | Explanation of why the error occurred.                        |
| Age         | Time the error has been in the error database.                |

The following example shows CFM IEEE sample output from a **show ethernet cfm errors** command using the optional **configuration** keyword:

```
Router# show ethernet cfm errors configuration
-----
CFM Interface      Type  Id    Level  Error type
-----
Et0/0              VLAN  100   1      CFMLeak
```

Table 20 describes the significant fields shown in the display.

**Table 20** *show ethernet cfm errors configuration Field Descriptions*

| Field         | Description                                          |
|---------------|------------------------------------------------------|
| CFM Interface | CFM supported interface on which the error occurred. |
| Type          | Type of MEP (VLAN or port MEP)                       |
| Id            | Identifier of the VLAN on which the error occurred.  |
| Level         | Maintenance level at which the error occurred.       |
| Error type    | Type of error.                                       |

The following example shows CFM D1 sample output from a **show ethernet cfm errors** command for CFM error conditions at maintenance level 3:

```
Router# show ethernet cfm errors level 3
```

```
Level Vlan MPID Remote MAC      Reason      Service ID
5      102   40 aabb.cc00.ca10    Receive AIS    service test
```

[Table 21](#) describes the significant fields shown in the display.

**Table 21** *show ethernet cfm errors Field Descriptions*

| Field      | Description                                                    |
|------------|----------------------------------------------------------------|
| Level      | Maintenance level at which the error occurred.                 |
| Vlan       | VLAN on which the error occurred.                              |
| MPID       | Identifier of the MEP on which the error occurred.             |
| Remote MAC | The MAC address of the remote MEP on which the error occurred. |
| Reason     | Explanation of why the error occurred.                         |
| Service ID | Identifier of the customer affected by the error.              |

# show ethernet cfm maintenance-points local

To display information about maintenance points configured on a device, use the **show ethernet cfm maintenance-points local** command in privileged EXEC mode.

**show ethernet cfm maintenance-points local** [**detail**] [**mep** | **mip**] [**domain** *domain-name* | **interface** *type number* | **level** *level-id*]

| Syntax Description |                                                                                |
|--------------------|--------------------------------------------------------------------------------|
| <b>detail</b>      | (Optional) Indicates that detailed output is specified.                        |
| <b>mep</b>         | (Optional) Indicates that a maintenance endpoint (MEP) is specified.           |
| <b>mip</b>         | (Optional) Indicates that a maintenance intermediate point (MIP) is specified. |
| <b>domain</b>      | (Optional) Indicates that a maintenance domain is specified.                   |
| <i>domain-name</i> | (Optional) String of a maximum of 154 characters.                              |
| <b>interface</b>   | (Optional) Indicates that an interface is specified.                           |
| <i>type number</i> | (Optional) Type and number of the interface.                                   |
| <b>level</b>       | (Optional) Indicates that a maintenance level is specified.                    |
| <i>level-id</i>    | (Optional) Integer from 0 to 7 that identifies the maintenance level.          |

**Command Default** When none of the optional keywords and arguments are specified, information about all the maintenance points on the device is shown.

**Command Modes** Privileged EXEC (#)

| Command History | Release      | Modification                                                                                                                                                                                              |
|-----------------|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.2(33)SRA  | This command was introduced.                                                                                                                                                                              |
|                 | 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T.                                                                                                                                             |
|                 | 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.                                                                                                                                           |
|                 | 12.2(33)SRD  | The <b>detail</b> and <b>evc</b> keywords and the <i>evc-name</i> argument were added.                                                                                                                    |
|                 | 12.2(33)SX12 | This command was integrated into Cisco IOS Release 12.2(33)SX12. <ul style="list-style-type: none"> <li>The <b>evc</b> keyword and <i>evc-name</i> argument are not supported in this release.</li> </ul> |
|                 | 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not support the <b>evc</b> parameter.                                                                                   |

**Usage Guidelines** The **show ethernet cfm maintenance-points local** command allows you to filter output. You can display information about maintenance points as follows:

- Independent of domain or interface
- On a particular interface independent of domain

- On a particular interface belonging to a given domain
- Belonging to a given domain independent of interface

The display may also be restricted to either MEPs or MIPs.

If a domain name has more than 43 characters, a warning message is displayed notifying that the maintenance domain ID (MDID) is truncated to 43 characters in continuity check messages (CCMs) if “id <fmt> <MDID>” is not configured.

## Examples

Following is sample output from a **show ethernet cfm maintenance-points local detail** command when none of the other optional keywords and arguments are specified:

```
Router# show ethernet cfm maintenance-points local detail
```

Local MEPs:

| MPID | Domain Name | Lvl | MacAddress     | Type | CC |
|------|-------------|-----|----------------|------|----|
|      | Domain Id   | Dir | Port           | Id   |    |
|      | MA Name     |     | SrvInst        |      |    |
|      | EVC name    |     |                |      |    |
| 301  | Domain_L7   | 7   | aabb.cc03.bb99 | Vlan | Y  |
|      | Domain_L7   | Up  | Et0/1          | 11   |    |
|      | cust_700_17 |     | N/A            |      |    |
|      | N/A         |     |                |      |    |
| 401  | Domain_L5   | 5   | aabb.cc03.bb99 | Vlan | Y  |
|      | Domain_L5   | Up  | Et0/1          | 9    |    |
|      | cust_500_15 |     | N/A            |      |    |
|      | N/A         |     |                |      |    |

Total Local MEPs: 2

Local MIPs: None

[Table 22](#) describes the significant fields shown in the display.

**Table 22** *show ethernet cfm maintenance-points local Field Descriptions*

| Field       | Description                                                  |
|-------------|--------------------------------------------------------------|
| MPID        | Identifier of the maintenance point.                         |
| Domain Name | Name of the domain.                                          |
| Lvl         | Maintenance level where the maintenance point is configured. |
| MacAddress  | MAC address of the maintenance point.                        |
| Type        | Type of MEP (VLAN or port MEP)                               |
| CC          | Continuity check operational status.                         |
| Domain Id   | Identifier of the domain.                                    |
| Dir         | Direction which the maintenance point is facing.             |
| Port        | Port MEP.                                                    |
| Id          | Identifier of the VLAN.                                      |
| MA Name     | Name of the maintenance association.                         |



**Table 22** *show ethernet cfm maintenance-points local Field Descriptions (continued)*

| Field    | Description                                 |
|----------|---------------------------------------------|
| SrvInst  | MAC address of the MEP.                     |
| EVC name | Name of the Ethernet virtual circuit (EVC). |

# show ethernet cfm maintenance-points remote

To display detailed information about remote maintenance endpoints (MEPs) configured statically in the MEP list and their status in the continuity check database (CCDB), use the **show ethernet cfm maintenance-points remote** command in privileged EXEC mode.



## Note

Release 12.2(33)MRA supports the Draft 1.0 version of Ethernet CFM; it does not support the IEEE 802.1ag-2007 version.

### Cisco pre-Standard Ethernet Connectivity Fault Management Draft 1 (CFM D1)

**show ethernet cfm maintenance-points remote** [**domain** *domain-name* | **level** *level-id*]

### CFM IEEE 802.1ag Standard (CFM IEEE)

**show ethernet cfm maintenance-points remote** [**domain** *domain-name* | [[**crosscheck** | **static**]  
[**domain** *domain-name* | **mpid** *mpid* [**domain** *domain-name*]] [**port** | **vlan** *vlan-id*]]]

## Syntax Description

|                    |                                                                                   |
|--------------------|-----------------------------------------------------------------------------------|
| <b>domain</b>      | (Optional) Indicates that a maintenance domain is specified.                      |
| <i>domain-name</i> | (Optional) String of a maximum of 154 characters.                                 |
| <b>level</b>       | (Optional) Indicates that a maintenance level is specified.                       |
| <i>level-id</i>    | (Optional) Integer from 0 to 7 that identifies the maintenance level.             |
| <b>crosscheck</b>  | (Optional) Shows the Mep-Up status from the D1 crosscheck function.               |
| <b>static</b>      | (Optional) Shows the Mep-Up status from the continuity-check static rmp function. |
| <b>mpid</b>        | (Optional) Shows a remote maintenance point.                                      |
| <i>mpid</i>        | (Optional) Integer from 0 to 8191 that identifies the maintenance point.          |
| <b>port</b>        | (Optional) Shows the operational state of the port MEP.                           |
| <b>vlan</b>        | (Optional) Shows a VLAN configuration.                                            |
| <i>vlan-id</i>     | (Optional) Integer from 1 to 4094 that identifies the VLAN.                       |

## Command Default

When neither a domain nor a level (CFM D1 only) is specified, all CCDB MEP entries are displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release     | Modification                                                                                               |
|-------------|------------------------------------------------------------------------------------------------------------|
| 12.2(33)SRA | This command was introduced.                                                                               |
| 12.4(11)T   | This command was integrated into Cisco IOS Release 12.4(11)T.                                              |
| 12.2(33)SRB | The output of this command was enhanced to include the port state values of REMOTE_EE, LOCAL_EE, and TEST. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH.                                            |

| Release      | Modification                                                     |
|--------------|------------------------------------------------------------------|
| 12.2(33)SX12 | This command was integrated into Cisco IOS Release 12.2(33)SX12. |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.  |

### Usage Guidelines

If a domain name has more than 43 characters, a warning message is displayed notifying that the maintenance domain ID (MDID) is truncated to 43 characters in continuity check messages (CCMs) if “id <fmt> <MDID>” is not configured.

When no maintenance domain is specified, all entries are displayed; otherwise only entries belonging to the specified domain or level (CFM D1 only) are shown.

### Examples

The following example shows output from a **show ethernet cfm maintenance-points remote** command:

```
Router# show ethernet cfm maintenance-points remote
```

| MPID | Domain Name | MacAddress     | IfSt     | PtSt |
|------|-------------|----------------|----------|------|
| Lvl  | Domain ID   | Ingress        |          |      |
| RDI  | MA Name     | Type Id        | SrvcInst |      |
|      | EVC Name    |                | Age      |      |
| 37   | Domain_port | aabb.cc03.ba00 | Up       | N/A  |
| 0    | Domain_port | Et0/0          |          |      |
| -    | portmep     | Port none      | N/A      |      |
|      | N/A         |                | 1s       |      |
| 401  | Domain_L5   | aabb.cc03.bb99 | Up       | Up   |
| 5    | Domain_L5   | Et0/0.9        |          |      |
| -    | cust_500_15 | Vlan 9         | N/A      |      |
|      | N/A         |                | 2s       |      |
| 301  | Domain_L7   | aabb.cc03.bb99 | Up       | Up   |
| 7    | Domain_L7   | Et0/0.11       |          |      |
| -    | cust_700_17 | Vlan 11        | N/A      |      |
|      | N/A         |                | 0s       |      |

Total Remote MEPS: 3

Table 23 describes the significant fields shown in the display.

**Table 23** *show ethernet cfm maintenance-points remote Field Descriptions*

| Field       | Description                                                       |
|-------------|-------------------------------------------------------------------|
| MPID        | Identifier of the MEP.                                            |
| Lvl         | Maintenance level.                                                |
| RDI         | Remote defect indication (RDI) messages on the maintenance point. |
| Domain Name | Name of the domain.                                               |
| Domain ID   | MAC address of the MEP.                                           |
| MA Name     | Name of the maintenance association.                              |
| EVC Name    | Identifier of the Ethernet virtual circuit (EVC).                 |
| Mac Address | MAC address of the MEP.                                           |

**Table 23** *show ethernet cfm maintenance-points remote Field Descriptions (continued)*

| Field   | Description                                                                                                                                                                                                                                          |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ingress | Port on which the packet is received.                                                                                                                                                                                                                |
| Type Id | Type of service.                                                                                                                                                                                                                                     |
| IfSt    | Operational state of the interface.                                                                                                                                                                                                                  |
| SrvInst | MAC address of the MEP.                                                                                                                                                                                                                              |
| Age     | Amount of time, in seconds, the entry has been in the database.                                                                                                                                                                                      |
| PtSt    | Operational state of the port MEP. Values are:<br>UP—Operational.<br>DOWN—Not operational.<br>ADMINDOWN—Administratively down.<br>REMOTE_EE—Encountered excessive remote errors.<br>LOCAL_EE—Encountered excessive local errors.<br>TEST—Test state. |

**Related Commands**

| Command                                                       | Description                                                                                       |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>show ethernet cfm maintenance-points local</b>             | Displays information about maintenance points configured on a device.                             |
| <b>show ethernet cfm maintenance-points remote crosscheck</b> | Displays information about remote maintenance points configured statically in a cross-check list. |
| <b>show ethernet cfm maintenance-points remote detail</b>     | Displays information about a remote maintenance point in the continuity check database.           |

# show ethernet cfm maintenance-points remote crosscheck

To display information about remote maintenance points configured statically in a cross-check list, use the **show ethernet cfm maintenance-points remote crosscheck** command in privileged EXEC mode.

**show ethernet cfm maintenance-points remote crosscheck** [**mpid** *id* | **mac** *mac-address*]  
[**domain** *domain-name* | **level** *level-id*] [**vlan** *vlan-id*]

| Syntax Description |                                                                                       |
|--------------------|---------------------------------------------------------------------------------------|
| <b>mpid</b>        | (Optional) Indicates that a maintenance domain is specified.                          |
| <i>id</i>          | (Optional) Integer from 0 to 8191 that identifies the maintenance domain.             |
| <b>mac</b>         | (Optional) Indicates that a maintenance domain is specified.                          |
| <i>mac-address</i> | (Optional) MAC address of the remote maintenance point, in the format abcd.abcd.abcd. |
| <b>domain</b>      | (Optional) Indicates that a maintenance domain is specified.                          |
| <i>domain-name</i> | (Optional) String of a maximum of 154 characters.                                     |
| <b>level</b>       | (Optional) Indicates that a maintenance level is specified.                           |
| <i>level-id</i>    | (Optional) Integer from 0 to 7 that identifies the maintenance level.                 |
| <b>vlan</b>        | (Optional) Indicates a VLAN for configuration.                                        |
| <i>vlan-id</i>     | (Optional) Integer value of 1 to 4094 that identifies the VLAN.                       |

**Command Default** When no options are specified, maintenance point IDs (MPIDs), MAC addresses, domains, levels, and VLANs for all maintenance points on the list are displayed.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification                                                                                                                                                                  |
|-----------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.2(33)SRA | This command was introduced.                                                                                                                                                  |
|                 | 12.4(11)T   | This command was integrated into Cisco IOS Release 12.4(11)T.                                                                                                                 |
|                 | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH.                                                                                                               |
|                 | 12.2(33)SRD | The <b>evc</b> keyword and <i>evc-name</i> argument were added on the Cisco 7600 Series Route Switch Processor 720 (RSP 720) and the Cisco 7600 Series Supervisor Engine 720. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not support the <b>evc</b> parameter.                                                       |

**Examples**

Following is sample output from a **show ethernet cfm maintenance-points remote crosscheck** command for maintenance points at maintenance level 4:

```
Router# show ethernet cfm maintenance-points remote crosscheck level 4
```

```
-----
MPID Level VLAN Mep-Up Remote Mac
-----
200  4      0    No    aabb.cc00.0310
-----
```

```
MPID Level Mep-Up Remote Mac
              EVC
-----
200  4      No    aabb.cc00.0310
              evc_100
```

Table 24 describes the significant fields shown in the display.

**Table 24** *show ethernet cfm maintenance-points remote crosscheck Field Descriptions*

| Field      | Description                                                  |
|------------|--------------------------------------------------------------|
| MPID       | Identifier of the maintenance point.                         |
| Level      | Maintenance level where the maintenance point is configured. |
| VLAN       | ID of the VLAN on which the maintenance point is configured. |
| Mep-Up     | Operational status of the MEP.                               |
| Remote Mac | MAC address of the remote maintenance point.                 |
| EVC        | ID of the EVC on which the maintenance point is configured.  |

**Related Commands**

| Command                                                   | Description                                                                             |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <b>show ethernet cfm maintenance-points local</b>         | Displays information about maintenance points configured on a device.                   |
| <b>show ethernet cfm maintenance-points remote</b>        | Displays information about remote maintenance points in the continuity check database.  |
| <b>show ethernet cfm maintenance-points remote detail</b> | Displays information about a remote maintenance point in the continuity check database. |

# show ethernet cfm maintenance-points remote detail

To display information about a remote maintenance point in the continuity check database, use the **show ethernet cfm maintenance-points remote detail** command in privileged EXEC mode.



## Note

Release 12.2(33)MRA supports the Draft 1.0 version of Ethernet CFM; it does not support the IEEE 802.1ag-2007 version.

### Cisco pre-Standard Connectivity Fault Management Draft 1 (CFM D1)

**show ethernet cfm maintenance-points remote detail** {**mac** *mac-address* | **mpid** *id*} [**domain** *domain-name* | **level** *level-id*] [**service** *service-name* | **vlan** *vlan-id*]

### CFM IEEE 802.1ag Standard (CFM IEEE)

**show ethernet cfm maintenance-points remote detail** {**mac** *mac-address* | **mpid** *id*} [**domain** *domain-name* [**port** | **vlan** *vlan-id*]]

## Syntax Description

|                     |                                                                            |
|---------------------|----------------------------------------------------------------------------|
| <b>mac</b>          | Shows a remote MAC address.                                                |
| <i>mac-address</i>  | MAC address of the remote maintenance point, in the format abcd.abcd.abcd. |
| <b>mpid</b>         | Shows a remote maintenance point.                                          |
| <i>id</i>           | Integer from 0 to 8191 that identifies the maintenance point.              |
| <b>domain</b>       | (Optional) Shows a specific maintenance domain.                            |
| <i>domain-name</i>  | (Optional) String of a maximum of 154 characters.                          |
| <b>level</b>        | (Optional) Shows a specific maintenance level.                             |
| <i>level-id</i>     | (Optional) Integer from 0 to 7 that identifies the maintenance level.      |
| <b>service</b>      | (Optional) Shows a customer service instance.                              |
| <i>service-name</i> | (Optional) String that identifies the service instance.                    |
| <b>port</b>         | (Optional) Shows the operational state of the port MEP.                    |
| <b>vlan</b>         | (Optional) Shows a VLAN configuration.                                     |
| <i>vlan-id</i>      | (Optional) Integer from 1 to 4094 that identifies the VLAN.                |

## Command Default

When no options are specified, all remote maintenance endpoints (MEPs) matching the specified MAC address or maintenance point ID (MPID) are displayed.

## Command Modes

Privileged EXEC (#)

**Command History**

| Release      | Modification                                                                                                                                                                           |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(33)SRA  | This command was introduced.                                                                                                                                                           |
| 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T.                                                                                                                          |
| 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.                                                                                                                        |
| 12.2(33)SRD  | Output was modified in Cisco IOS Release 12.2(33)SRD to show detailed information about Receive RDI and EVC. The <b>evc</b> keyword and <i>evc-name</i> argument were also introduced. |
| 12.2(33)SXI2 | This command was integrated into Cisco IOS Release 12.2(33)SXI2.                                                                                                                       |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA. This release does not support the <b>evc</b> parameter.                                                                |

**Usage Guidelines**

Use this command to obtain information about a specific maintenance point by specifying its MPID or to obtain information about all maintenance points that have a particular MAC address.

When a maintenance domain is not specified, all matching maintenance points, independent of their levels (CFM D1 only), are displayed; otherwise, only maintenance points at the specified maintenance domain are shown.

In CFM D1 only, when an EVC is specified, only maintenance points that are members of the EVC are displayed.

When a VLAN is specified, only maintenance points on that VLAN are displayed.

**Examples**

The following is sample output from a **show ethernet cfm maintenance-points remote detail** command using the **mpid** option:

```
Router# show ethernet cfm maintenance-points remote detail mpid 401

Version: IEEE-CFM
MAC Address: aabb.cc03.bb99
Domain Name: Domain_L5
MA Name: cust_500_15
Level: 5
VLAN: 9
MPID: 401
Sender Chassis ID: Router3-cfm
Incoming Port(s): Ethernet0/0.9
CC Lifetime(sec): 35
Age of Last CC Message(sec): 10
CC Packet Statistics: 91/0 (Received/Error)
MEP interface status: Up
MEP port status: Up
Receive RDI: FALSE
Router#
```

Table 25 describes the significant fields shown in the display.

**Table 25** *show ethernet cfm maintenance-points remote detail Field Descriptions*

| Field       | Description                     |
|-------------|---------------------------------|
| Version     | Version of CFM that is running. |
| MAC Address | MAC address of the remote MEP   |



**Table 25** *show ethernet cfm maintenance-points remote detail Field Descriptions (continued)*

| Field                       | Description                                                                                       |
|-----------------------------|---------------------------------------------------------------------------------------------------|
| Domain Name                 | Name of the domain.                                                                               |
| MA Name                     | Name of the maintenance association.                                                              |
| Level                       | Maintenance domain level.                                                                         |
| VLAN                        | Configured VLAN.                                                                                  |
| MPID                        | Identifier of the maintenance point.                                                              |
| Sender Chassis ID           | Name of the other switch or router when sender-id is configured on that device.                   |
| Incoming Port(s)            | Identifier of the port that receives the message.                                                 |
| CC Lifetime(sec)            | Amount of time, in seconds, that the message should remain in the database before being purged.   |
| Age of Last CC Message(sec) | Amount of time, in seconds, the previous continuity check message (CCM) has been in the database. |
| CC Packet Statistics        | Number of packets received and number of packets with errors.                                     |
| MEP interface status        | Operational state of the MEP interface.                                                           |
| MEP port status             | Operational state of the MEP port.                                                                |
| Receive RDI                 | Receive status of remote defect indication (RDI) messages on the maintenance point.               |

**Related Commands**

| Command                                                       | Description                                                                                       |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>show ethernet cfm maintenance-points local</b>             | Displays information about maintenance points configured on a device.                             |
| <b>show ethernet cfm maintenance-points remote</b>            | Displays information about remote maintenance points in the continuity check database.            |
| <b>show ethernet cfm maintenance-points remote crosscheck</b> | Displays information about remote maintenance points configured statically in a cross-check list. |

# show ethernet cfm statistics

To display Ethernet connectivity fault management (CFM) information, use the **show ethernet cfm statistics** command in privileged EXEC mode.

**show ethernet cfm statistics** [**domain** [*domain-name* [**service** {*ma-name* | *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*}] | **mpid** *mpid*]

| Syntax Description |                                                                          |
|--------------------|--------------------------------------------------------------------------|
| <b>domain</b>      | (Optional) Configures a maintenance domain.                              |
| <i>domain-name</i> | (Optional) String of a maximum of 154 characters.                        |
| <b>service</b>     | (Optional) Configures a maintenance association within the domain.       |
| <i>ma-name</i>     | (Optional) String that identifies the maintenance association.           |
| <i>ma-num</i>      | (Optional) Integer that identifies the maintenance association.          |
| <b>vlan-id</b>     | (Optional) Configures a VLAN.                                            |
| <i>vlan-id</i>     | (Optional) Integer from 1 to 4094 that identifies the VLAN.              |
| <b>vpn-id</b>      | (Optional) Configures a virtual private network (VPN).                   |
| <i>vpn-id</i>      | (Optional) Integer from 1 to 32767 that identifies the VPN.              |
| <b>mpid</b>        | (Optional) Configures a maintenance point identifier.                    |
| <i>mpid</i>        | (Optional) Integer from 1 to 8191 that identifies the maintenance point. |

**Command Default** All domains are displayed when none of the keywords or arguments are selected.

**Command Modes** Privileged EXEC (#)

| Command History | Release      | Modification                                                    |
|-----------------|--------------|-----------------------------------------------------------------|
|                 | 12.2(33)SX12 | This command was introduced.                                    |
|                 | 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** Use this command to display an overview of transmitted and received messages.

If a domain name has more than 43 characters, a warning message is displayed notifying that the maintenance domain ID (MDID) is truncated to 43 characters in continuity check messages (CCMs) if “id <fmt> <MDID>” is not configured.

**Examples** Following is sample output from a **show ethernet cfm statistics** command:

```
Router# show ethernet cfm statistics

BRAIN MAC: aabb.cc03.b999

DomainName: Domain_L7
MA Name: cust_700_17
```

```

MPID: 101
  Last clearing of counters: never
  CCMs:
    Transmitted:          242    Rcvd Seq Errors:      0
  LTRs:
    Unexpected Rcvd:      0
  LBRs:
    Transmitted:          0    Rcvd Seq Errors:      0
    Rcvd in order:        0    Rcvd Bad MSDU:        0

DomainName: Domain_L5
MA Name: cust_500_15
MPID: 220
  Last clearing of counters: never
  CCMs:
    Transmitted:          202    Rcvd Seq Errors:      0
  LTRs:
    Unexpected Rcvd:      0
  LBRs:
    Transmitted:          0    Rcvd Seq Errors:      0
    Rcvd in order:        10    Rcvd Bad MSDU:        0

DomainName: Domain_port
MA Name: portmep
MPID: 112
  Last clearing of counters: never
  CCMs:
    Transmitted:          278    Rcvd Seq Errors:      0
  LTRs:
    Unexpected Rcvd:      0
  LBRs:
    Transmitted:          0    Rcvd Seq Errors:      0
    Rcvd in order:        0    Rcvd Bad MSDU:        0

```

Table 26 describes the significant fields shown in the display.

**Table 26** *show ethernet cfm statistics Field Descriptions*

| Field      | Description                            |
|------------|----------------------------------------|
| BRAIN MAC  | Bridge brain MAC address.              |
| DomainName | Domain name.                           |
| MA Name    | Maintenance association name.          |
| MPID       | Maintenance point identifier.          |
| CCMs       | Continuity check messages transmitted. |
| LTRs       | Linktrace responses.                   |
| LBRs       | Loopback responses.                    |

# show ethernet cfm traceroute-cache

To display the contents of the traceroute cache, use the **show ethernet cfm traceroute-cache** command in privileged EXEC mode.

**show ethernet cfm traceroute-cache**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

| Command History | Release      | Modification                                                     |
|-----------------|--------------|------------------------------------------------------------------|
|                 | 12.2(33)SRA  | This command was introduced.                                     |
|                 | 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T.    |
|                 | 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.  |
|                 | 12.2(33)SXI2 | This command was integrated into Cisco IOS Release 12.2(33)SXI2. |
|                 | 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.  |

**Usage Guidelines** Use the **show ethernet cfm traceroute-cache** command to display the contents of the traceroute cache; for example, to see the maintenance intermediate points (MIPs) and maintenance endpoints (MEPs) of a domain as they were discovered. The data is historic. The traceroute cache stores entries from previous traceroute operations.

**Examples** The following example shows output from a **show ethernet cfm traceroute-cache** command:

```
Router# show ethernet cfm traceroute-cache
```

```
Traceroute to aabb.cc03.b999 on Domain Domain_L5, Level 5, vlan 9 issued at 01:25:22
path found via MPDB
```

```
B = Intermediary Bridge
! = Target Destination
* = Per hop Timeout
```

```
-----
Hops      Host                MAC              Ingress      Ingr Action  Relay Action
          Host                Forwarded      Egress      Egr Action  Previous Hop
-----
! 1                aabb.cc03.b999
          Not Forwarded                                RlyHit:MEP
  aabb.cc03.bb99
```

Table 27 describes the significant fields shown in the display.

**Table 27** *show ethernet cfm traceroute-cache Field Descriptions*

| Field        | Description                                                                                                      |
|--------------|------------------------------------------------------------------------------------------------------------------|
| Hops         | Number of hops of the traceroute.                                                                                |
| Host         | Name of the device.                                                                                              |
| MAC          | Bridge Brain MAC address of the device.                                                                          |
| Ingress      | Receiving port.                                                                                                  |
| Ingr Action  | Action on the ingress port: IngOk, IngFilter, IngBlocked.                                                        |
| Relay Action | Type of relay action performed: RlyNone, RlyUnknown, RlyFDB, RlyCCDB, RlyFiltered.                               |
| Forwarded    | Traceroute forwarded or not forwarded.                                                                           |
| Egress       | Sending port.                                                                                                    |
| Egr Action   | Action on the egress port: EgrNone, EgrTTL, EgrDown, EgrBlocked, EgrOk, EgrGVRP, EgrDomainBoundary, EgrFiltered. |
| Previous Hop | MAC address of the neighboring device.                                                                           |

#### Related Commands

| Command                                    | Description                                                               |
|--------------------------------------------|---------------------------------------------------------------------------|
| <b>clear ethernet cfm traceroute-cache</b> | Removes the contents of the traceroute cache.                             |
| <b>ethernet cfm traceroute-cache</b>       | Enables caching of Ethernet CFM data learned through traceroute messages. |
| <b>traceroute ethernet</b>                 | Sends Ethernet CFM traceroute messages to a destination MAC address.      |

# show ethernet lmi

To display Ethernet local management interface (LMI) Ethernet virtual connections (EVCs) configured on a device, use the **show ethernet lmi** command in privileged EXEC mode.

```
show ethernet lmi {{ evc [detail evc-id [interface type number] | map interface type number]} |
                  {parameters | statistics} interface type number | uni map [interface type number]}
```

## Syntax Description

|                   |                                                                                                                                                                                                                                                                                                                       |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>evc</b>        | Displays information about an EVC.                                                                                                                                                                                                                                                                                    |
| <b>detail</b>     | (Optional) Displays detailed information about a specified EVC.                                                                                                                                                                                                                                                       |
| <i>evc-id</i>     | (Optional) String of a maximum of 100 characters that identifies an EVC.                                                                                                                                                                                                                                              |
| <b>interface</b>  | Indicates that an interface is specified. This keyword is optional except with the <b>parameters</b> and <b>statistics</b> keywords.                                                                                                                                                                                  |
| <i>type</i>       | String that identifies the type of interface. Valid options are the following: <ul style="list-style-type: none"> <li><b>ethernet</b>—Ethernet IEEE 802.3 interface</li> <li><b>fastethernet</b>—Fast Ethernet IEEE 802.3 interface</li> <li><b>gigabitethernet</b>—Gigabit Ethernet IEEE 802.3z interface</li> </ul> |
| <i>number</i>     | Integer that identifies the interface.                                                                                                                                                                                                                                                                                |
| <b>map</b>        | (Optional) Indicates a VLAN map.                                                                                                                                                                                                                                                                                      |
| <b>parameters</b> | Displays Ethernet LMI parameters.                                                                                                                                                                                                                                                                                     |
| <b>statistics</b> | Displays Ethernet LMI statistics.                                                                                                                                                                                                                                                                                     |
| <b>uni map</b>    | Displays information about the user-network interface (UNI).                                                                                                                                                                                                                                                          |

## Command Modes

Privileged EXEC (#)

## Command History

| Release     | Modification                                                                                         |
|-------------|------------------------------------------------------------------------------------------------------|
| 12.4(9)T    | This command was introduced.                                                                         |
| 12.2(33)SRB | Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                      |

## Usage Guidelines

Use this command to check the operational statuses of EVCs.

**Examples**

The following examples show output from a **show ethernet lmi** command for interface Ethernet 0/0 using different keywords and arguments.

The following sample output is generated from the **show ethernet lmi** command using the **evc** keyword:

```
Router# show ethernet lmi evc
```

```
St   EVC Id                                     Port
-----
A   EVC_MP2MP_101                             Gi0/1
A   EVC_P2P_110                               Gi0/1
```

Key: St=Status, A=Active, P=Partially Active, I=Inactive, ?=Link Down

The following sample output is generated from the **show ethernet lmi** command using the **evc** and optional **detail** keywords:

```
Router# show ethernet lmi evc detail EVC_MP2MP_101
```

```
EVC Id: EVC_MP2MP_101
interface Ethernet0/0
  Time since Last Full Report: 00:25:25
  Ether LMI Link Status: Up
  UNI Status: Up
  UNI Id: router3-e0/0+router-e0/0
  CE-VLAN/EVC Map Type: Bundling
  VLAN: 101

  EVC Status: Active
  EVC Type: Multipoint-to-Multipoint
  Remote UNI Count: Configured = 2, Active = 2

  UNI Id                                     UNI Status   Port
  ----
  router4-e0/0+router1-e0/0                 Up            Remote
  router5-e0/0+router6-e0/0                 Up            Remote
```

Table 28 describes the significant fields shown in output of the **show ethernet lmi** command using the **evc** and **detail** keywords.

**Table 28** *show ethernet lmi evc detail Field Descriptions*

| Field                       | Description                                                                 |
|-----------------------------|-----------------------------------------------------------------------------|
| EVC Id                      | Identifier of the EVC.                                                      |
| Time since Last Full Report | Number of hours, minutes, seconds since the CE requested a detailed report. |
| Ether LMI Link Status       | Operational state of the LMI link.                                          |
| UNI Status                  | Operational state of the UNI.                                               |
| UNI Id                      | Identifier of the UNI between the CE and PE devices.                        |
| CE-VLAN/EVC Map Type        | EVC map type: bundling, multiplex, or all-to-one                            |
| VLAN                        | Identifier of the VLAN.                                                     |
| EVC Status                  | Operational state of the EVC.                                               |
| EVC Type                    | Type of connection (point-to-point or multipoint-to-multipoint).            |

**Table 28** *show ethernet lmi evc detail Field Descriptions (continued)*

| Field            | Description                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------|
| Remote UNI Count | Number of remote UNIs that are configured and the number that are operational.                                             |
| Port             | Type of port, either local or remote, on which the EVC is configured. If the port is local, the interface ID is specified. |

The following sample output is generated from the **show ethernet lmi** command using the **map interface** keyword:

```
Router# show ethernet lmi evc map interface Ethernet0/0
```

```
UNI Id: router3-e0/0+router-e0/0
St  Evc Id                               CE-VLAN
-----
  A  EVC_MP2MP_101                       101
  A  EVC_P2P_110                         110
```

Key: St=Status, A=Active, P=Partially Active, I=Inactive, \*=Default EVC,  
?=Link Down

[Table 29](#) describes the significant fields shown in output of the **show ethernet lmi** command using the **evc** and **map** keywords.

**Table 29** *show ethernet lmi evc map Field Descriptions*

| Field   | Description                                          |
|---------|------------------------------------------------------|
| UNI Id  | Identifier of the UNI between the CE and PE devices. |
| St      | Operational state of the EVC.                        |
| Evc Id  | Identifier of the EVC.                               |
| CE-VLAN | Identifier of the VLAN used by the CE.               |

The following sample output is generated from the **show ethernet lmi** command using the **parameters** and **interface** keywords:

```
Router# show ethernet lmi parameters interface Ethernet0/0
```

```
E-LMI Parameters for interface Ethernet0/0
Version : MEF.16-0106
Mode : CE
T391 : 10
T392 : NA
N391 : 360
N393 : 4
```

[Table 30](#) describes the significant fields shown in output of the **show ethernet lmi** command using the **parameters** keyword.



**Table 30** *show ethernet lmi parameters Field Descriptions*

| Field   | Description                                                                |
|---------|----------------------------------------------------------------------------|
| Version | Version number of the specification that E-LMI implementation is based on. |
| Mode    | Customer equipment or the Metro Ethernet network.                          |
| T391    | Polling timer.                                                             |
| T392    | Polling verification timer.                                                |
| N391    | Polling counter.                                                           |
| N393    | Event counter.                                                             |

The following sample output is generated from the **show ethernet lmi** command using the **statistics** and **interface** keywords:

```
Router# show ethernet lmi statistics interface Ethernet0/0

E-LMI Statistics for interface Ethernet0/0
  Ether LMI Link Status: Up
  UNI Status: Up
  UNI Id: router3-e0/0+router-e0/0

Reliability Errors:
  Status Timeouts          0  Invalid Sequence Number      0
  Invalid Status Response   0  Unsolicited Status Received  0

Protocol Errors:
  Invalid Protocol Version   0  Invalid EVC Reference Id     0
  Invalid Message Type       0  Out of Sequence IE           0
  Duplicated IE              0  Mandatory IE Missing         0
  Invalid Mandatory IE       0  Invalid non-Mandatory IE     0
  Unrecognized IE            0  Unexpected IE                 0
  Short Message              0

Last Full Status Enq Sent    00:50:35  Last Full Status Rcvd       00:50:35
Last Status Check Sent      00:00:06  Last Status Check Rcvd      00:00:06
Last clearing of counters    00:09:57
```



**Note** The UNI Id field displays only when it is available from the provider edge router.

[Table 31](#) describes the significant fields shown in output of the **show ethernet lmi** command using the **statistics** keyword.

**Table 31** *show ethernet lmi statistics Field Descriptions*

| Field                                                      | Description                                     |
|------------------------------------------------------------|-------------------------------------------------|
| <b>E-LMI Statistics for interface &lt;interface-id&gt;</b> |                                                 |
| Ether LMI Link Status                                      | Operational state of Ethernet LMI connectivity. |
| UNI Status                                                 | Operational state of the UNI.                   |
| UNI Id                                                     | Identifier of the UNI.                          |
| <b>Reliability Errors</b>                                  |                                                 |

**Table 31** *show ethernet lmi statistics Field Descriptions (continued)*

| Field                       | Description                                                                                                             |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Status Timeouts             | Number of times that a status request has been sent but not received.                                                   |
| Invalid Sequence Number     | Number of times the sequence numbers of Ethernet LMI packets do not match the sequence numbers expected.                |
| Invalid Status Response     | Number of times a status response received was invalid and discarded.                                                   |
| Unsolicited Status Received | Number of times status was received that had not been requested.                                                        |
| <b>Protocol Errors</b>      |                                                                                                                         |
| Invalid Protocol Version    | Number of times the protocol version in Ethernet LMI packets does not match what is supported.                          |
| Invalid EVC Reference Id    | Number of times EVC reference IDs are invalid in Ethernet LMI packets.                                                  |
| Invalid Message Type        | Number of message types that are not valid for LMI.                                                                     |
| Out of Sequence IE          | Number of information elements (IEs) that are not in the correct sequence.                                              |
| Duplicated IE               | Number of duplicated IEs.                                                                                               |
| Mandatory IE Missing        | Number of mandatory IEs that are missing.                                                                               |
| Invalid Mandatory IE        | Number of mandatory IEs that are invalid.                                                                               |
| Invalid non-Mandatory IE    | Number of non-mandatory IEs that are invalid.                                                                           |
| Unrecognized IE             | Number of IEs that are not recognized.                                                                                  |
| Unexpected IE               | Number of IEs that are unexpected.                                                                                      |
| Short Message               | Number of times the Ethernet LMI message received is shorter than supported packets.                                    |
| Last Full Status Enq Sent   | Time in hours, minutes, and seconds when the CE sent the last full LMI status request.                                  |
| Last Full Status Rcvd       | Time in hours, minutes, and seconds when the CE received the last full LMI status report.                               |
| Last Status Check Sent      | Time in hours, minutes, and seconds when the CE sent the last LMI status request.                                       |
| Last Status Check Rcvd      | Time in hours, minutes, and seconds when the CE received the last LMI status report.                                    |
| Last clearing of counters   | Time in hours, minutes, and seconds when the clear <b>ethernet lmi statistics</b> command was issued for the interface. |

The following sample output is generated from the **show ethernet lmi** command using the **uni map** keyword:

```
Router# show ethernet lmi uni map
```

|              |               |       |
|--------------|---------------|-------|
| UNI Id       | EVC Id        | Port  |
| -----        | -----         | ----- |
| uni_sandiego | EVC_MP2MP_101 | Gi0/1 |

```
uni_sandiego          EVC_P2P_110          Gi0/1
Router#
```

The following sample output is generated from the **show ethernet lmi** command using the **uni map** and optional **interface** keywords:

```
Router# show ethernet lmi uni map interface gigabitethernet 0/1

UNI Id          EVC Id          Port
-----
uni_sandiego    EVC_MP2MP_101   Gi0/1
uni_sandiego    EVC_P2P_110     Gi0/1
Router#
```

Table 32 describes the significant fields shown in output of the **show ethernet lmi** command using the **uni map** keyword and **uni map** and **interface** keyword pair.

**Table 32** *show ethernet lmi uni map and uni map interface Field Descriptions*

| Field  | Description                 |
|--------|-----------------------------|
| UNI Id | Identifier of the UNI.      |
| EVC Id | Identifier of the EVC.      |
| Port   | Interface on the CE device. |

# show ethernet oam discovery

To display discovery information for all Ethernet operations, maintenance, and administration (OAM) interfaces or for a specific interface, use the **show ethernet oam discovery** command in privileged EXEC mode.

**show ethernet oam discovery** [*interface type number*]

|                           |                  |                                                                                                             |
|---------------------------|------------------|-------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>interface</b> | (Optional) Specifies an interface.                                                                          |
|                           | <i>type</i>      | (Optional) Type of Ethernet interface. Valid values are: FastEthernet, GigabitEthernet, TenGigabitEthernet. |
|                           | <i>number</i>    | (Optional) Integer from 1 to 9 that is the number of the Ethernet interface.                                |

|                      |                     |
|----------------------|---------------------|
| <b>Command Modes</b> | Privileged EXEC (#) |
|----------------------|---------------------|

|                        |                |                                                                 |
|------------------------|----------------|-----------------------------------------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                             |
|                        | 12.2(33)SRA    | This command was introduced.                                    |
|                        | 12.4(15)T      | This command was integrated into Cisco IOS Release 12.4(15)T.   |
|                        | 12.2(33)SXH    | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** This command displays the following information pertaining to Ethernet OAM discovery:

- Remote device which is directly connected to this device
- Local and remote OAM configuration and capability
- Local and remote OAM mode
- Remote platform identity
- State of the local discovery state machine

If an interface is specified, only data pertaining to the OAM peer on that interface is displayed; otherwise, data for all OAM peers (on all interfaces) is displayed.

**Examples** The following example shows output from a **show ethernet oam discovery** command for interface GigabitEthernet 6/11:

```
Router# show ethernet oam discovery interface gigabitethernet6/11

GigabitEthernet6/11
Local client
-----
Administrative configurations:
  Mode:                active
  Unidirection:        not supported
  Link monitor:        supported (on)
  Remote loopback:     supported
```

```

MIB retrieval:      not supported
Mtu size:           1500
Operational status:
  Port status:      operational
  Loopback status:  no loopback
  PDU revision:     1

Remote client
-----
MAC address: 0030.96fd.6bfa
Vendor(oui): 0x00 0x00 0x0C (cisco)

Administrative configurations:
  Mode:             active
  Unidirection:     not supported
  Link monitor:     supported
  Remote loopback:  supported
  MIB retrieval:    not supported
  Mtu size:         1500

```

Table 33 describes the significant fields shown in the display.

**Table 33** *show ethernet oam discovery Field Descriptions*

| Field                                | Description                                                                                      |
|--------------------------------------|--------------------------------------------------------------------------------------------------|
| <b>Administrative configurations</b> |                                                                                                  |
| Mode                                 | Active or passive mode of the interface                                                          |
| Unidirection                         | Operational mode                                                                                 |
| Link monitor                         | Status of link monitor support                                                                   |
| Remote loopback                      | Status of remote loopback support                                                                |
| MIB retrieval                        | Capability of requesting MIB objects.                                                            |
| Mtu size                             | Size of the maximum transmission unit                                                            |
| <b>Operational status</b>            |                                                                                                  |
| Port status                          | Operational state of the port                                                                    |
| Loopback status                      | Operational status of the loopback interface                                                     |
| PDU revision                         | Revision of the OAM configuration. A new revision results from each change to the configuration. |
| <b>Remote client</b>                 |                                                                                                  |
| MAC address                          | MAC address of the remote client                                                                 |
| Vendor (oui)                         | Vendor number in hexadecimal                                                                     |

| Related Commands | Command                             | Description                                                                          |
|------------------|-------------------------------------|--------------------------------------------------------------------------------------|
|                  | <b>show ethernet oam statistics</b> | Displays detailed information about Ethernet OAM packets.                            |
|                  | <b>show ethernet oam status</b>     | Displays Ethernet OAM configurations for all interfaces or for a specific interface. |
|                  | <b>show ethernet oam summary</b>    | Displays active Ethernet OAM sessions.                                               |

# show ethernet oam statistics

To display detailed information about Ethernet operations, maintenance, and administration (OAM) packets, use the **show ethernet oam statistics** command in privileged EXEC mode.

**show ethernet oam statistics** [*interface type number*]

| Syntax Description | interface     | (Optional) Specifies an interface.                                                                          |
|--------------------|---------------|-------------------------------------------------------------------------------------------------------------|
|                    | <i>type</i>   | (Optional) Type of Ethernet interface. Valid values are: FastEthernet, GigabitEthernet, TenGigabitEthernet. |
|                    | <i>number</i> | (Optional) Integer from 1 to 9 that is the number of the Ethernet interface.                                |

| Command Modes | Privileged EXEC (#) |
|---------------|---------------------|
|---------------|---------------------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(33)SRA | This command was introduced.                                    |
|                 | 12.4(15)T   | This command was integrated into Cisco IOS Release 12.4(15)T.   |
|                 | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** Statistics that this command displays include the following:

- Rx/Tx OAM Protocol Data Unit (PDU) counters
- Link monitoring events, including event logs, if available
- Remote fault detection events
- Remote loopback events

## Examples

The following example shows output from a **show ethernet oam statistics** command for interface GigabitEthernet 6/11:

```
Router# show ethernet oam statistics interface gigabitethernet 6/11
```

```
GigabitEthernet6/11
```

```
Counters:
```

```
-----
```

```

Information OAMPDU Tx           : 9723
Information OAMPDU Rx           : 9712
Unique Event Notification OAMPDU Tx : 0
Unique Event Notification OAMPDU Rx : 0
Duplicate Event Notification OAMPDU TX : 0
Duplicate Event Notification OAMPDU RX : 0
Loopback Control OAMPDU Tx      : 0
Loopback Control OAMPDU Rx      : 0
Variable Request OAMPDU Tx      : 0
Variable Request OAMPDU Rx      : 0
Variable Response OAMPDU Tx     : 0
```

## show ethernet oam statistics

```

Variable Response OAMPDU Rx          : 0
Cisco OAMPDU Tx                      : 0
Cisco OAMPDU Rx                      : 0
Unsupported OAMPDU Tx                 : 0
Unsupported OAMPDU Rx                 : 0
Frames Lost due to OAM                : 0

Local event logs:
-----
 0 Errored Symbol Period records
 0 Errored Frame records
 0 Errored Frame Period records
 0 Errored Frame Second records

Remote event logs:
-----
 0 Errored Symbol Period records
 0 Errored Frame records
 0 Errored Frame Period records
 0 Errored Frame Second records

```

Table 34 describes the significant fields shown in the display.

**Table 34** *show ethernet oam statistics Field Descriptions*

| Field                                  | Description                                                                               |
|----------------------------------------|-------------------------------------------------------------------------------------------|
| <b>Counters</b>                        |                                                                                           |
| Information OAMPDU Tx                  | Number of OAM PDUs transmitted                                                            |
| Information OAMPDU Rx                  | Number of OAM PDUs received                                                               |
| Unique Event Notification OAMPDU Tx    | Number of unique event notification OAM PDUs transmitted                                  |
| Unique Event Notification OAMPDU Rx    | Number of unique event notification OAM PDUs received                                     |
| Duplicate Event Notification OAMPDU Tx | Number of duplicate event notification OAM PDUs transmitted                               |
| Duplicate Event Notification OAMPDU Rx | Number of duplicate event notification OAM PDUs received                                  |
| Loopback Control OAMPDU Tx             | Number of loopback control OAM PDUs transmitted                                           |
| Loopback Control OAMPDU Rx             | Number of loopback control OAM PDUs received                                              |
| Variable Request OAMPDU Tx             | Number of OAM PDUs sent to request MIB objects on a remote device                         |
| Variable Request OAMPDU Rx             | Number of OAM PDUs received and requesting MIB objects on a local device                  |
| Variable Response OAMPDU Tx            | Number of OAM PDUs sent by the local device in response to a request from a remote device |
| Variable Response OAMPDU Rx            | Number of OAM PDUs sent by the remote device in response to a request from a local device |
| Cisco OAMPDU Tx                        | Number of Cisco specific OAM PDUs sent                                                    |
| Cisco OAMPDU Rx                        | Number of Cisco specific OAM PDUs received                                                |
| Unsupported OAMPDU Tx                  | Number of unsupported OAM PDUs sent                                                       |



**Table 34** *show ethernet oam statistics Field Descriptions (continued)*

| Field                  | Description                                  |
|------------------------|----------------------------------------------|
| Unsupported OAMPDU Rx  | Number of unsupported OAM PDUs received      |
| Frames lost due to OAM | Number of frames discarded by the OAM client |
| Local event logs       | Log of events on the local device            |
| Remote event logs      | Log of events on the remote device           |

**Related Commands**

| Command                            | Description                                                                                 |
|------------------------------------|---------------------------------------------------------------------------------------------|
| <b>show ethernet oam discovery</b> | Displays discovery information for all Ethernet OAM interfaces or for a specific interface. |
| <b>show ethernet oam status</b>    | Displays Ethernet OAM configurations for all interfaces or for a specific interface.        |
| <b>show ethernet oam summary</b>   | Displays active Ethernet OAM sessions.                                                      |

# show ethernet oam status

To display Ethernet operations, maintenance, and administration (OAM) configurations for all interfaces or for a specific interface, use the **show ethernet oam status** command in privileged EXEC mode.

**show ethernet oam status** [*interface type number*]

|                           |                  |                                                                                                             |
|---------------------------|------------------|-------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>interface</b> | (Optional) Specifies an interface.                                                                          |
|                           | <i>type</i>      | (Optional) Type of Ethernet interface. Valid values are: FastEthernet, GigabitEthernet, TenGigabitEthernet. |
|                           | <i>number</i>    | (Optional) Integer from 1 to 9 that is the number of the Ethernet interface.                                |

|                      |                     |
|----------------------|---------------------|
| <b>Command Modes</b> | Privileged EXEC (#) |
|----------------------|---------------------|

|                        |                |                                                                 |
|------------------------|----------------|-----------------------------------------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                             |
|                        | 12.2(33)SRA    | This command was introduced.                                    |
|                        | 12.4(15)T      | This command was integrated into Cisco IOS Release 12.4(15)T.   |
|                        | 12.2(33)SXH    | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                                                                                                                                |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | Use this command to display the runtime settings of link-monitoring and general OAM operations for all interfaces or for a specific interface. |
|                         | OAM must be operational on the interface or interfaces before you issue this command.                                                          |

|                 |                                                                                                                       |
|-----------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | The following example shows output from a <b>show ethernet oam status</b> command for interface GigabitEthernet 6/11: |
|                 | Router# <b>show ethernet oam status interface gigabitethernet 6/11</b>                                                |

```
GigabitEthernet6/11
General
-----
Mode:                active
PDU max rate:        10 packets per second
PDU min rate:        1 packet per 1 second
Link timeout:        5 seconds
High threshold action: no action

Link Monitoring
-----
Status: supported (on)

Symbol Period Error
Window:              1 million symbols
Low threshold:       1 error symbol(s)
```

```

High threshold:      none

Frame Error
Window:              10 x 100 milliseconds
Low threshold:       1 error frame(s)
High threshold:      none

Frame Period Error
Window:              1 x 100,000 frames
Low threshold:       1 error frame(s)
High threshold:      none

Frame Seconds Error
Window:              600 x 100 milliseconds
Low threshold:       1 error second(s)
High threshold:      none

```

Table 35 describes the significant fields shown in the display.

**Table 35** *show ethernet oam status Field Descriptions*

| Field                      | Description                                                          |
|----------------------------|----------------------------------------------------------------------|
| <b>General</b>             |                                                                      |
| Mode                       | Active or passive mode of the interface.                             |
| PDU max rate               | Maximum number of protocol data units (PDUs) transmitted per second. |
| PDU min rate               | Minimum number of PDUs transmitted per second.                       |
| Link timeout               | Amount of time with inactivity before the link is dropped.           |
| High threshold action      | Action that occurs when the high threshold for an error is exceeded. |
| <b>Link Monitoring</b>     |                                                                      |
| Status                     | Operational state of the port.                                       |
| <b>Symbol Period Error</b> |                                                                      |
| Window                     | Specified number of error symbols.                                   |
| Low threshold              | Minimum number of error symbols.                                     |
| High threshold             | Maximum number of error symbols.                                     |
| <b>Frame Error</b>         |                                                                      |
| Window                     | Specified amount of time in milliseconds.                            |
| Low threshold              | Minimum number of error frames.                                      |
| High threshold             | Maximum number of error frames.                                      |
| <b>Frame Period Error</b>  |                                                                      |
| Window                     | Frequency at which the measurement is taken, in milliseconds.        |
| Low threshold              | Minimum number of error frames.                                      |
| High threshold             | Maximum number of error frames.                                      |
| <b>Frame Seconds Error</b> |                                                                      |

**Table 35** *show ethernet oam status Field Descriptions (continued)*

| Field          | Description                                                   |
|----------------|---------------------------------------------------------------|
| Window         | Frequency at which the measurement is taken, in milliseconds. |
| Low threshold  | Lowest value at which an event is triggered.                  |
| High threshold | Highest value at which an event is triggered.                 |

**Related Commands**

| Command                             | Description                                                                                 |
|-------------------------------------|---------------------------------------------------------------------------------------------|
| <b>show ethernet oam discovery</b>  | Displays discovery information for all Ethernet OAM interfaces or for a specific interface. |
| <b>show ethernet oam statistics</b> | Displays detailed information about Ethernet OAM packets.                                   |
| <b>show ethernet oam summary</b>    | Displays active Ethernet OAM sessions.                                                      |

# show ethernet oam summary

To display active Ethernet operations, maintenance, and administration (OAM) sessions on a device, use the **show ethernet oam summary** command in privileged EXEC mode.

## show ethernet oam summary

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(33)SRA | This command was introduced.                                    |
|                 | 12.4(15)T   | This command was integrated into Cisco IOS Release 12.4(15)T.   |
|                 | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Examples** The following example shows output from a **show ethernet oam summary** command:

```
Router# show ethernet oam summary
```

```
Symbols:          * - Master Loopback State, # - Slave Loopback State
Capability codes: L - Link Monitor, R - Remote Loopback
                  U - Unidirection, V - Variable Retrieval
```

| Local Interface | MAC Address    | Remote Vendor | Mode   | Capability |
|-----------------|----------------|---------------|--------|------------|
| Fa3/1           | 0080.09ff.e4a0 | 00000C        | active | L R        |
| Gi6/11          | 0030.96fd.6bfa | 00000C        | active | L R        |

Table 36 describes the significant fields shown in the display.

**Table 36** *show ethernet oam summary Field Descriptions*

| Field           | Description                               |
|-----------------|-------------------------------------------|
| Local Interface | Type of local interface                   |
| MAC Address     | MAC address of the local interface        |
| Remote Vendor   | The vendor for the remote device.         |
| Mode            | Operational state of the local interface  |
| Capability      | Functions the local interface can perform |

| Related Commands | Command                             | Description                                                                                 |
|------------------|-------------------------------------|---------------------------------------------------------------------------------------------|
|                  | <b>show ethernet oam discovery</b>  | Displays discovery information for all Ethernet OAM interfaces or for a specific interface. |
|                  | <b>show ethernet oam statistics</b> | Displays detailed information about Ethernet OAM packets.                                   |
|                  | <b>show ethernet oam status</b>     | Displays Ethernet OAM configurations for all interfaces or for a specific interface.        |

# show interfaces rep

Use the **show interfaces rep** User EXEC command to display Resilient Ethernet Protocol (REP) configuration and status for a specified interface or for all interfaces.

**show interfaces** [*interface-id*] **rep** [**detail**] [ | { **begin** | **exclude** | **include** } *expression*]

## Syntax Description

|                     |                                                                                                        |
|---------------------|--------------------------------------------------------------------------------------------------------|
| <i>interface-id</i> | (Optional) Display REP configuration and status for a specified physical interface or port channel ID. |
| <b>detail</b>       | (Optional) Display detailed REP configuration and status information.                                  |
| <b>begin</b>        | (Optional) Displays output beginning with the line that matches the <i>expression</i> .                |
| <b>exclude</b>      | (Optional) Displays output that excludes lines that match the <i>expression</i> .                      |
| <b>include</b>      | (Optional) Displays output that includes lines that match the specified <i>expression</i> .            |
| <i>expression</i>   | Expression in the output to use as a reference point.                                                  |

## Command Modes

User EXEC

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(40)SE  | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

In the output for the **show interface rep [detail]** command, in addition to an *Open*, *Fail*, or AP (alternate port) state, the Port Role might show as *Fail Logical Open* (*FailLogOpen*) or *Fail No Ext Neighbor* (*FailNoNbr*). These states indicate that the port is physically up, but REP is not configured on the neighboring port. In this case, one port goes into a forwarding state for the data path to help maintain connectivity during configuration. The Port Role for this port shows as *Fail Logical Open*; the port forwards all data traffic on all VLANs. The other failed Port Role shows as *Fail No Ext Neighbor*; this port blocks traffic for all VLANs.

When the external neighbors for the failed ports are configured, the failed ports go through the alternate port state transitions and eventually go to an *Open* state or remain as the alternate port, based on the alternate port election mechanism.

The output of this command is also included in the **show tech-support** privileged EXEC command output.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

**Examples**

This is sample output from the **show interface rep** command:

```
Switch # show interface rep
Interface          Seg-id  Type      LinkOp  Role
-----
GigabitEthernet 0/1      1      Primary Edge TWO_WAY  Open
GigabitEthernet 0/2      1      Edge      TWO_WAY  Open
FastEthernet 0/4        2              INIT_DOWN Fail
```

This is sample output from the **show interface rep** command when the edge port is configured to have no REP neighbor. Note the asterisk (\*) next to *Primary Edge*.

```
Router# show interface rep
Interface          Seg-id  Type      LinkOp  Role
-----
GigabitEthernet0/1      2              TWO_WAY  Open
GigabitEthernet0/2      2      Primary Edge* TWO_WAY  Open
```

This is sample output from the **show interface rep** command when external neighbors are not configured:

```
Switch # show interface rep
Interface          Seg-id  Type      LinkOp  Role
-----
GigabitEthernet0/1      1              NO_NEIGHBOR FailNoNbr
GigabitEthernet0/2      2              NO_NEIGHBOR FailLogOpen
```

This is sample output from the **show interface rep detail** command for a specified interface:

```
Switch # show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2  REP enabled
Segment-id: 1 (Segment)
PortID: 00030019E85BDD00
Preferred flag: No
Operational Link Status: INIT_DOWN
Current Key: 00000000000000000000
Port Role: Fail
Blocked VLAN: 1-4094
Admin-vlan: 1
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: 1234567890123456
Configured Load-balancing Block VLAN: 1-4094
STCN Propagate to: none
LSL PDU rx: 0, tx: 0
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

**Related Commands**

| Command                                    | Description                                                                                                                                                    |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">rep segment</a>                | Enables REP on an interface and assigns a segment ID. This command is also used to configure a port as an edge port, a primary edge port, or a preferred port. |
| <a href="#">show rep topology [detail]</a> | Displays information about all ports in the segment, including which one was configured and selected as the primary edge port.                                 |



# show interface switchport backup

Displays status information about the backup switchport.

## show interface switchport backup

**Command Modes** Privileged EXEC

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(19)MR2 | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Examples

The following example shows the output generated by this command:

```
Router# show interface switchport backup
```

```
Switch Backup Interface Pairs:
```

| Active Interface   | Backup Interface   | State                   |
|--------------------|--------------------|-------------------------|
| -----              |                    |                         |
| GigabitEthernet0/0 | GigabitEthernet0/5 | Active Down/Backup Down |

| Related Commands | Command                     | Description                         |
|------------------|-----------------------------|-------------------------------------|
|                  | switchport backup interface | Configures a backup interface pair. |

# show ip mroute

To display the contents of the multicast routing (mroute) table, use the show ip mroute command in user EXEC or privileged EXEC mode.



## Note

The Cisco MWR 2941 only supports multicast routing for PTP redundancy. For more information, see the [“Configuring Pseudowire-based Clocking with Adaptive Clock Recovery”](#) section on page 4-45.

```
show ip mroute [vrf vrf-name] [[active [kbps] [interface type number] | bidirectional | count
[terse] | dense | interface type number | proxy | pruned | sparse | ssm | static | summary] |
[group-address [source-address]] [count [terse] | interface type number | proxy | pruned |
summary] | [source-address group-address] [count [terse] | interface type number | proxy |
pruned | summary] | [group-address] active [kbps] [interface type number]]
```

## Syntax Description

|                              |                                                                                                                                                                                                                                               |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vrf vrf-name</b>          | (Optional) Filters the output to display only the contents of the mroute table that pertain to the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRP) instance specified for the vrf-name argument.                       |
| <b>active kbps</b>           | (Optional) Displays the rate that active sources are sending to multicast groups, in kilobits per second (kbps). Active sources are those sending at the kbps value or higher. The range is from 1 to 4294967295. The kbps default is 4 kbps. |
| <b>interface type number</b> | (Optional) Filters the output to display only mroute table information related to the interface specified for the type number arguments.                                                                                                      |
| <b>bidirectional</b>         | (Optional) Filters the output to display only information about bidirectional routes in the mroute table.                                                                                                                                     |
| <b>count</b>                 | (Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bytes per second.                                                                                        |
| <b>terse</b>                 | (Optional) Filters the output to display a subset of mroute statistics, excluding source and group statistics for each mroute entry in the mroute table.                                                                                      |
| <b>dense</b>                 | (Optional) Filters the output to display only information about dense mode routes in the mroute table.                                                                                                                                        |
| <b>proxy</b>                 | (Optional) Displays information about Reverse Path Forwarding (RPF) vector proxies received on a multicast router.                                                                                                                            |
| <b>pruned</b>                | (Optional) Filters the output to display only information about pruned routes in the mroute table.                                                                                                                                            |
| <b>sparse</b>                | (Optional) Filters the output to display only information about sparse mode routes in the mroute table.                                                                                                                                       |
| <b>ssm</b>                   | (Optional) Filters the output to display only the Source Specific Multicast (SSM) routes in the mroute table.                                                                                                                                 |
| <b>static</b>                | (Optional) Filters the output to display only the static routes in the mroute table.                                                                                                                                                          |
| <b>summary</b>               | (Optional) Filters the output to display a one-line, abbreviated summary of each entry in the mroute table.                                                                                                                                   |

|                       |                                                                              |
|-----------------------|------------------------------------------------------------------------------|
| <i>group-address</i>  | (Optional) IP address or Domain Name System (DNS) name of a multicast group. |
| <i>source-address</i> | (Optional) IP address or DNS name of a multicast source.                     |

**Command Modes**

User EXEC, Privileged EXEC

**Command History**

| Release      | Modification                                                                                                                                                                                                             |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.0         | This command was introduced.                                                                                                                                                                                             |
| 12.0(5)T     | The H flag for multicast multilayer switching (MMLS) was added in the output display.                                                                                                                                    |
| 12.1(3)T     | The U, s, and I flags for Source Specific Multicast (SSM) were introduced.                                                                                                                                               |
| 12.0(23)S    | The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.                                                                                                                                                          |
| 12.0(30)S    | The <b>proxy</b> keyword, and the v and V flags were added for the Multicast VPN Inter-AS Support feature.                                                                                                               |
| 12.2(13)T    | The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.                                                                                                                                                          |
| 12.2(14)S    | This command was integrated into Cisco IOS Release 12.2(14)S. The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.                                                                                            |
| 12.3         | The Z, Y, and y flags were introduced.                                                                                                                                                                                   |
| 12.2(27)SBC  | This command was integrated into Cisco IOS Release 12.2(27)SBC.                                                                                                                                                          |
| 12.4(6)T     | The <b>terse</b> keyword was added.                                                                                                                                                                                      |
| 12.4(7)      | The <b>terse</b> keyword was added.                                                                                                                                                                                      |
| 12.2(18)SXF2 | The <b>terse</b> keyword was added.                                                                                                                                                                                      |
| 12.2(33)SRA  | This command was integrated into Cisco IOS Release 12.2(33)SRA. The <b>terse</b> keyword was added. The <b>proxy</b> keyword, and the v and V flags were added for the Multicast VPN Inter-AS Support feature.           |
| 12.2(31)SB2  | The E flag for the Multicast VPN Extranet Support feature was introduced. The <b>proxy</b> keyword, and the v and V flags were added for the Multicast VPN Inter-AS Support feature. The <b>terse</b> keyword was added. |
| 12.2(33)SXH  | The <b>proxy</b> keyword, and the v and V flags were added for the Multicast VPN Inter-AS Support feature.                                                                                                               |
| 12.2(33)SRC  | The E flag for the Multicast VPN Extranet Support feature was introduced.                                                                                                                                                |
| 12.4(20)T    | The <b>proxy</b> keyword, and the v and V flags were added for the Multicast VPN Inter-AS Support feature.                                                                                                               |
| 12.4(20)MR   | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                                                           |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                                                          |

**Usage Guidelines**

Use the **show ip mroute** command to display information about mroute entries in the mroute table. The Cisco IOS software populates the multicast routing table by creating (S, G) entries from (\*, G) entries. The asterisk (\*) refers to all source addresses, the "S" refers to a single source address, and the "G" is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (that is, through Reverse Path Forwarding [RPF]).

Use the **clear ip mroute** command to delete entries from the mroute table.

**Examples**

The following is sample output from the **show ip mroute** command for a router operating in sparse mode:

```
Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.3), uptime 5:29:15, RP is 192.168.37.2, flags: SC
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57

(192.168.46.0, 224.0.255.3), uptime 5:29:15, expires 0:02:59, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57
```

The following is sample output from the **show ip mroute** command with the IP multicast group address 232.6.6.6 specified:

```
Router# show ip mroute 232.6.6.6

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 232.6.6.6), 00:01:20/00:02:59, RP 224.0.0.0, flags: sSJP
  Incoming interface: Null, RPF nbr 224.0.0.0
  Outgoing interface list: Null

(10.2.2.2, 232.6.6.6), 00:01:20/00:02:59, flags: CTI
  Incoming interface: Ethernet3/3, RPF nbr 224.0.0.0
  Outgoing interface list:
    Ethernet3/1, Forward/Sparse-Dense, 00:00:36/00:02:35
```

The following is sample output from the **show ip mroute** command for a router operating in dense mode. This output displays the contents of the IP multicast routing table for the multicast group named cbone-audio.

```
Router# show ip mroute cbone-audio

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
```

```

Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.1), uptime 0:57:31, expires 0:02:59, RP is 224.0.0.0, flags: DC
  Incoming interface: Null, RPF neighbor 224.0.0.0, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Dense, 0:57:31/0:02:52
    Tunnel0, Forward/Dense, 0:56:55/0:01:28

(192.168.37.100, 224.0.255.1), uptime 20:20:00, expires 0:02:55, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.20.37.33, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Dense, 20:20:00/0:02:52

```

The following is sample output from the **show ip mroute** command that shows the virtual circuit descriptor (VCD) value, because an ATM interface with Protocol Independent Multicast (PIM) multipoint signaling is enabled:

```

Router# show ip mroute 224.1.1.1

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.1.1.1), 00:03:57/00:02:54, RP 172.16.0.0, flags: SJ
  Incoming interface: Null, RPF nbr 224.0.0.0224.0.0.0
  Outgoing interface list:
    ATM0/0, VCD 14, Forward/Sparse, 00:03:57/00:02:53

```

For more information about the **show ip mroute** command, see the *Cisco IOS IP Multicast Command Reference*.

| Related Commands | Command                | Description                            |
|------------------|------------------------|----------------------------------------|
|                  | <b>clear ip mroute</b> | Deletes entries from the mroute table. |

# show mpls l2transport vc

To display information about Any Transport over MPLS (AToM) virtual circuits (VCs) that have been enabled to route Layer 2 packets on a router, use the **show mpls l2transport vc** command in privileged EXEC mode.

**show mpls l2transport vc** [**vcid** *vc-id*] | [**vcid** *vc-id-min vc-id-max*] } [**interface** *name* [*local-circuit-id*]] [**destination** *ip-address* | *name*] [**detail**]

| Syntax Description                   |                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vcid</b>                          | (Optional) Allows you to enter a specific VC ID to display.                                                                                                                                                                                                                                                                                                           |
| <i>vc-id</i>                         | (Optional) The VC ID number.                                                                                                                                                                                                                                                                                                                                          |
| <i>vc-id-min</i><br><i>vc-id-max</i> | (Optional) Range of VCs to display. The range is from 1 to 4294967295. (This argument is primarily used for legacy implementations.)                                                                                                                                                                                                                                  |
| <b>interface</b>                     | (Optional) The interface or subinterface of the router that has been enabled to transport Layer 2 packets. This keyword lets you display information about the VCs that have been assigned VC IDs on that interface or subinterface.                                                                                                                                  |
| <i>name</i>                          | (Optional) Name of the interface or subinterface.                                                                                                                                                                                                                                                                                                                     |
| <i>local-circuit-id</i>              | (Optional) Number assigned to the local circuit. This argument value is supported only by the following transport types: <ul style="list-style-type: none"> <li>For ATM adaptation layer 5 (AAL5) and cell relay, enter the virtual path identifier (VPI)/virtual channel identifier (VCI) of the PVC.</li> <li>For Ethernet VLANs, enter the VLAN number.</li> </ul> |
| <b>destination</b>                   | (Optional) Displays information about the VCs that have been assigned VC IDs for the remote router you specify.                                                                                                                                                                                                                                                       |
| <i>ip-address</i>                    | (Optional) IP address of the remote router.                                                                                                                                                                                                                                                                                                                           |
| <i>name</i>                          | (Optional) Name assigned to the remote router.                                                                                                                                                                                                                                                                                                                        |
| <b>detail</b>                        | (Optional) Displays detailed information about the VCs that have been assigned VC IDs.                                                                                                                                                                                                                                                                                |

**Command Modes** Privileged EXEC

| Command History | Release    | Modification                                                     |
|-----------------|------------|------------------------------------------------------------------|
|                 | 12.1(8a)E  | This command was introduced.                                     |
|                 | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST.   |
|                 | 12.0(22)S  | This command was implemented on the Cisco 10720 router.          |
|                 | 12.0(23)S  | The <b>interface</b> and <b>destination</b> keywords were added. |
|                 | 12.2(14)S  | This command was integrated into Cisco IOS Release 12.2(14)S.    |
|                 | 12.2(14)SX | This command was implemented on the Supervisor Engine 720.       |
|                 | 12.2(14)SZ | This command was integrated into Cisco IOS Release 12.2(14)SZ.   |
|                 | 12.2(15)T  | This command was integrated into Cisco IOS Release 12.2(15)T.    |
|                 | 12.2(18)S  | This command was implemented on Cisco 7304 routers.              |

| Release      | Modification                                                                                                                                                                                                                                                                                                                              |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(25)S    | This command was updated with new output and fields to display information about tunnel selection and ATM cell relay port mode.                                                                                                                                                                                                           |
| 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.                                                                                                                                                                                                                                                 |
| 12.2(25)S    | This command was updated with new output and fields for nonstop forwarding (NSF), stateful switchover (SSO), and graceful restart (GR) abilities.                                                                                                                                                                                         |
| 12.2(28)SB   | This command was implemented on the Cisco 10000 series routers. Example output was changed for the Cisco 10000 series router, and two fields (SSO Descriptor and SSM segment/switch IDs) were removed from the output, because they are not supported.                                                                                    |
| 12.2(33)SRA  | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                                                                                                                                                                           |
| 12.2(33)SRB  | This command was updated to include forwarding equivalence class (FEC) 129 signaling information for pseudowires that are configured through VPLS Autodiscovery, and to support provisioning Any Transport over MPLS (AToM) static pseudowires.                                                                                           |
| 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.                                                                                                                                                                                                                                                                           |
| 12.2(33)SRC  | This command was updated to display the number of MAC address withdrawal messages sent and received as part of the H-VPLS N-PE Redundancy for QinQ and MPLS Access feature.<br><br>This command was updated to display pseudowire status between peer routers that have been configured for the MPLS Pseudowire Status Signaling feature. |
| 12.4(19)MR2  | This command was integrated into Cisco IOS Release 12.4(19)MR2.                                                                                                                                                                                                                                                                           |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                                                                                                                                                                           |

### Usage Guidelines

If you do not specify any keywords or arguments, the command displays a summary of all the VCs.

### Examples

The output of the commands varies, depending on the type of Layer 2 packets being transported over the AToM VCs.

The following example shows information about the interfaces and VCs that have been configured to transport various Layer 2 packets on the router:

Router# **show mpls l2transport vc**

| Local intf | Local circuit  | Dest address | VC ID | Status |
|------------|----------------|--------------|-------|--------|
| AT4/0      | ATM AAL5 0/100 | 10.0.0.1     | 100   | UP     |
| AT4/0      | ATM AAL5 0/200 | 10.0.0.1     | 200   | UP     |
| AT4/0.300  | ATM AAL5 0/300 | 10.0.0.1     | 300   | UP     |

Table B-37 describes the significant fields shown in the display.

**Table B-37** *show mpls l2transport vc Field Descriptions*

| Field         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Local intf    | The interface on the local router that has been enabled to transport Layer 2 packets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Local circuit | The type and number (if applicable) of the local circuit. The output shown in this column varies, depending on the transport type: <ul style="list-style-type: none"> <li>For ATM cell relay and AAL5, the output shows the VPI/VCI of the PVC.</li> <li>For Ethernet VLANs, the output shows the VLAN number.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Dest address  | The IP address of the remote router's interface that is the other end of the VC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| VC ID         | The VC identifier assigned to one of the interfaces on the router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Status        | The status of the VC. The status can be one of the following conditions: <ul style="list-style-type: none"> <li>UP—The VC is in a state where it can carry traffic between the two VC endpoints. A VC is up when both imposition and disposition interfaces are programmed. <ul style="list-style-type: none"> <li>The disposition interface is programmed if the VC has been configured and the client interface is up.</li> <li>The imposition interface is programmed if the disposition interface is programmed and you have a remote VC label and an Interior Gateway Protocol (IGP) label. The IGP label can be implicit null in a back-to-back configuration. An IGP label means there is a Label Switched Path (LSP) to the peer.</li> </ul> </li> <li>DOWN—The VC is not ready to carry traffic between the two VC endpoints. Use the <b>detail</b> keyword to determine the reason that the VC is down.</li> <li>ADMIN DOWN—The VC has been disabled by a user.</li> <li>RECOVERING—The VC is recovering from a stateful switchover.</li> </ul> |

The following example shows information about the NSF/SSO and graceful restart capability. The SSO portion indicates when checkpointing data has either been sent (on active) or received (on standby). When SSO data has not been successfully sent or has been released, the SSO information is not shown.

Router# **show mpls l2transport vc detail**

```

Local interface: Fa0/1.1 down, line protocol down, Eth VLAN 2 up
Destination address: 10.55.55.2, VC ID: 1002, VC status: down
Output interface: Fa0/0, imposed label stack {16}
Preferred path: not configured
Default path: active
Tunnel label: imp-null, next hop point2point
Create time: 02:03:29, last status change time: 02:03:26
Signaling protocol: LDP, peer 10.55.55.2:0 down
MPLS VC labels: local 16, remote unassigned
Group ID: local 0, remote unknown
MTU: local 1500, remote unknown
Remote interface description:
Sequencing: receive disabled, send disabled
SSO Descriptor: 10.55.55.2/1002, local label: 16
SSM segment/switch IDs: 12290/8193, PWID: 8193
VC statistics:

```



```

packet totals: receive 0, send 0
byte totals:   receive 0, send 0
packet drops:  receive 0, send 0

```

Table B-38 describes the significant fields shown in the display.

**Table B-38** *show mpls l2transport vc Field Descriptions*

| Field                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Local interface         | Interface on the local router that has been enabled to send and receive Layer 2 packets. The interface varies, depending on the transport type. The output also shows the status of the interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| line protocol           | Status of the line protocol on the edge-facing interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Destination address     | IP address of the remote router specified for this VC. Specify the destination IP address as part of the <b>mpls l2transport route</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| VC ID                   | VC identifier assigned to the interface on the router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| VC status               | <p>Status of the VC, which is one of the following conditions:</p> <p>UP—The VC is in a state where it can carry traffic between the two VC endpoints. A VC is up when both imposition and disposition interfaces are programmed.</p> <ul style="list-style-type: none"> <li>The disposition interface is programmed if the VC has been configured and the client interface is up.</li> <li>The imposition interface is programmed if the disposition interface is programmed and a remote VC label and an IGP label exist. The IGP label can be an implicit null in a back-to-back configuration. (An IGP label means there is an LSP to the peer.)</li> </ul> <p>DOWN—The VC is not ready to carry traffic between the two VC endpoints.</p> <p>ADMIN DOWN—The VC has been disabled by a user.</p> |
| Output interface        | Interface on the remote router that has been enabled to transmit and receive Layer 2 packets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| imposed label stack     | Summary of the MPLS label stack used to direct the VC to the PE router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Preferred path          | Path that was assigned to the VC and the status of that path. The path can be an MPLS traffic engineering tunnel or an IP address or hostname of a PE router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Default path            | <p>Status of the default path, which can be disabled or active.</p> <p>By default, if the preferred path fails, the router uses the default path. However, you can disable the router from using the default path when the preferred path fails by specifying the <b>disable-fallback</b> keyword with the <b>preferred-path</b> command.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Create time             | Time when the VC was provisioned.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| last status change time | Last time the VC state changed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Signaling protocol      | Type of protocol used to send the MPLS labels. The output also shows the status of the peer router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| MPLS VC labels          | Local VC label is a disposition label, which determines the egress interface of an arriving packet from the MPLS backbone. The remote VC label is a disposition VC label of the remote peer router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Table B-38** *show mpls l2transport vc Field Descriptions (continued)*

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group ID                     | Local group ID is used to group VCs locally. The remote group ID is used by the peer to group several VCs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| MTU                          | Maximum transmission unit specified for the local and remote interfaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Remote interface description | Interface on the remote router that has been enabled to transmit and receive Layer 2 packets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Sequencing                   | Indicates whether sequencing of out-of-order packets is enabled or disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Tunnel label                 | <p>IGP label used to route the packet over the MPLS backbone to the destination router with the egress interface. The first part of the output displays the type of label. The second part of the output displays the route information.</p> <p>The tunnel label information can display any of the following states:</p> <ul style="list-style-type: none"> <li>• imp-null—The provider (P) router is absent and the tunnel label is not to be used. Alternatively, imp-null can signify traffic engineering tunnels between the PE routers.</li> <li>• unassigned—The label has not been assigned.</li> <li>• no route—The label is not in the routing table.</li> <li>• no adjacency—The adjacency for the next hop is missing.</li> <li>• not ready, no route—An IP route for the peer does not exist in the routing table.</li> <li>• not ready, not a host table—The route in the routing table for the remote peer router is not a host route.</li> <li>• not ready, Cisco Express Forwarding disabled—Cisco Express Forwarding is disabled.</li> <li>• not ready, label forwarding information base (LFIB) disabled—The MPLS switching subsystem is disabled.</li> <li>• not ready, LFIB entry present—The tunnel label exists in the LFIB, but the VC is down.</li> </ul> |
| SSO Descriptor               | The VC for which the information was checkpointed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| local label                  | The value of the local label that was checkpointed (that is, sent on the active Route Processor [RP], and received on the standby RP).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SSM segment/switch IDs       | The IDs used to refer to the control plane and data plane contexts for this VC. This data is not for customer use but for Cisco personnel for troubleshooting purposes. When the source specific multicast (SSM) IDs are followed by the word “used,” the checkpointed data has been successfully sent and not released.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| PWID                         | The PW ID used in the data plane to correlate the switching context for the segment mentioned with the MPLS switching context. This data is not for customer use but for Cisco personnel for troubleshooting purposes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| packet totals                | Number of packets sent and received. Received packets are those AToM packets received from the MPLS core. Sent packets are those AToM packets sent to the MPLS core. This number does not include dropped packets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| byte totals                  | Number of bytes sent and received from the core-facing interface, including the payload, control word if present, and AToM VC label.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Table B-38** *show mpls l2transport vc Field Descriptions (continued)*

| Field        | Description                |
|--------------|----------------------------|
| packet drops | Number of dropped packets. |

**Related Commands**

| Command                              | Description                                                                                              |
|--------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>show mpls l2transport summary</b> | Displays summary information about VCs that have been enabled to route AToM Layer 2 packets on a router. |

# show network-clocks

To display information about the network clocks configured on the router, use the **show network-clocks** command. The command shows the priority and state of all configured clocks and the currently selected clock.

**show network-clocks**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

| Command History | Release      | Modification                                                                                                                                                                      |
|-----------------|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 11.1         | This command was introduced.                                                                                                                                                      |
|                 | 12.2(33)SRA  | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2SX       | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                 | 12.2(33)SRD1 | This command was modified to display BITS clock information for the 7600-ES+ITU-2TG and the 7600-ES+ITU-4TG.                                                                      |
|                 | 12.4(19)MR2  | This command was integrated into Cisco IOS Release 12.4(19)MR2.                                                                                                                   |
|                 | 12.2(33)MRA  | This command was enhanced to show information for REP.                                                                                                                            |

**Examples** The following example shows how to use the **show network-clocks** command:

```
Router# show network-clocks
```

## Network Clock Configuration

| Priority | Source        | Status | Type          | Selected |
|----------|---------------|--------|---------------|----------|
| 01       | Packet Timing | NOT OK | Packet Timing | N        |
| 02       | E1 0/15       | OK     | E1/T1         | Y        |
| 03       | BITS          | NOT OK | BITS          | N        |
| 04       | E1 0/14       | OK     | E1/T1         | N        |

```
Current Clock State LOCK
clock input Stratum level: 3
```

```
mode : Revertive
```

```
hold-timeout 900 sec
```

| Related Commands | Command                                      | Description                                                 |
|------------------|----------------------------------------------|-------------------------------------------------------------|
|                  | <b>set network-clocks<br/>force-reselect</b> | This command causes the router to reselect a network clock. |

# show platform hardware

To display the status of hardware devices on the Cisco MWR 2941, use the **show platform hardware** command. The command displays information about hardware devices on the Cisco MWR 2941 for troubleshooting and debugging purposes.

**show platform hardware {adrian | bits | cpld | cpu | ethernet | fio | hwic | rtm | stratum | ufe  
winpath}**

## Syntax Description

|                 |                                                                           |
|-----------------|---------------------------------------------------------------------------|
| <b>adrian</b>   | Displays information about the adrian hardware.                           |
| <b>bits</b>     | Displays information about the BITS hardware.                             |
| <b>cpld</b>     | Displays information about the CPLD hardware.                             |
| <b>cpu</b>      | Displays information about the CPU.                                       |
| <b>ethernet</b> | Displays information about the ethernet interfaces on the Cisco MWR 2941. |
| <b>fio</b>      | Displays information about the FIO fpga hardware.                         |
| <b>hwic</b>     | Displays information about the HWICs installed on the Cisco MWR 2941.     |
| <b>rtm</b>      | Displays information about the RTM Module (ASM-M2900-TOP daughter card).  |
| <b>stratum</b>  | Displays information about the stratum hardware.                          |
| <b>ufe</b>      | Displays information about the UFE hardware.                              |
| <b>winpath</b>  | Displays information about the Winpath hardware.                          |

## Command Modes

Privileged EXEC

## Command History

| Release     | Modification                                                      |
|-------------|-------------------------------------------------------------------|
| 12.4(19)MR2 | This command was incorporated.                                    |
| 12.4(20)MR  | This command was modified to include PTP phase state information. |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.   |

## Examples

```
Router# show platform hardware rtm
ASM-M2900-TOP is OPERATIONAL
  CPLD version: 2.1(D)
Timing over Packet software running
  hybrid state: WAIT_FOR_NEW_PHASE
    protocol:      PTP version 2 (flags = 0x00000860)
    slave mode:    multicast hybrid
    local IP:      192.168.99.99 mask 255.255.255.0
    MAC address:   001e.bdff.759c
    ARP failures:  0
System timestamp using network clock driven hardware RTC
```

| Related Commands | Command         | Description                                |
|------------------|-----------------|--------------------------------------------|
|                  | show controller | Displays the status of system controllers. |

# show policy-map

To display the configuration of all classes for a specified service policy map or of all classes for all existing policy maps, use the **show policy-map** command in user EXEC or privileged EXEC mode.

**show policy-map** [*policy-map*]

|                           |                   |                                                                                                                                        |
|---------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>policy-map</i> | (Optional) Name of the service policy map whose complete configuration is to be displayed. The name can be a maximum of 40 characters. |
|---------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------|

|                        |                                                       |
|------------------------|-------------------------------------------------------|
| <b>Command Default</b> | All existing policy map configurations are displayed. |
|------------------------|-------------------------------------------------------|

|                      |                                      |
|----------------------|--------------------------------------|
| <b>Command Modes</b> | User EXEC (>)<br>Privileged EXEC (#) |
|----------------------|--------------------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | 12.0(5)T       | This command was introduced.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                        | 12.0(5)XE      | This command was incorporated into Cisco IOS Release 12.0(5)XE.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                        | 12.0(7)S       | This command was incorporated into Cisco IOS Release 12.0(7)S.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                        | 12.1(1)E       | This command was incorporated into Cisco IOS Release 12.1(1)E.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                        | 12.2(4)T       | This command was modified for two-rate traffic policing to display burst parameters and associated actions.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                        | 12.2(8)T       | The command was modified for the Policer Enhancement—Multiple Actions feature and the Weighted Random Early Detection (WRED)—Explicit Congestion Notification (ECN) feature.                                                                                                                                                                                                                                                                                                                                                                           |
|                        | 12.2(13)T      | The following modifications were made: <ul style="list-style-type: none"> <li>The output was modified for the Percentage-Based Policing and Shaping feature.</li> <li>This command was modified as part of the Modular QoS CLI (MQC) Unconditional Packet Discard feature. Traffic classes can now be configured to discard packets belonging to a specified class.</li> <li>This command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values.</li> </ul> |
|                        | 12.2(15)T      | This command was modified to support display of Frame Relay voice-adaptive traffic-shaping information.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|                        | 12.0(28)S      | The output of this command was modified for the QoS: Percentage-Based Policing feature to display the committed (conform) burst (bc) and excess (peak) burst (be) sizes in milliseconds (ms).                                                                                                                                                                                                                                                                                                                                                          |
|                        | 12.2(14)SX     | Support for this command was introduced on the Supervisor Engine 720.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                        | 12.2(17d)SXB   | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.                                                                                                                                                                                                                                                                                                                                                                                                                                            |



| Release          | Modification                                                                                                                                                                                                                                            |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(28)SB       | This command was integrated into Cisco IOS Release 12.2(28)SB, and the command was modified to display information about Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunnel marking.                                                                     |
| 12.2(31)SB2      | This command was enhanced to display bandwidth-remaining ratios configured on traffic classes and ATM overhead accounting, and was implemented on the Cisco 10000 series router for the PRE3.                                                           |
| 12.2(33)SRA      | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                                                                                         |
| 12.2(33)SRC      | Support for the Cisco 7600 series router was added.                                                                                                                                                                                                     |
| 12.4(15)T2       | This command was modified to display information about Generic Routing Encapsulation (GRE) tunnel marking.<br><br><b>Note</b> For this release, GRE-tunnel marking is supported on the Cisco MGX Route Processor Module (RPM-XF) platform <i>only</i> . |
| 12.2(33)SB       | This command was modified to display information about GRE-tunnel marking, and support for the Cisco 7300 series router was added. This command's output was modified on the Cisco 10000 series router for the PRE3 and PRE4.                           |
| Cisco IOS XE 2.1 | This command was integrated into Cisco IOS XE Release 2.1 and was implemented on the Cisco ASR 1000 series router.                                                                                                                                      |
| 12.4(20)T        | Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).                                                                                                              |
| 12.4(20)MR       | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                                                                                          |
| 12.2(33)MRA      | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                                                                                         |

### Usage Guidelines

The **show policy-map** command displays the configuration of a policy map created using the **policy-map** command. You can use the **show policy-map** command to display all class configurations comprising any existing service policy map, whether or not that policy map has been attached to an interface. The command displays:

- ECN marking information only if ECN is enabled on the interface.
- Bandwidth-remaining ratio configuration and statistical information, if configured and used to determine the amount of unused (excess) bandwidth to allocate to a class queue during periods of congestion.

### Examples

This section provides sample output from typical **show policy-map** commands. Depending upon the interface or platform in use and the options enabled (for example, Weighted Fair Queueing [WFQ]), the output you see may vary slightly from the ones shown below.

- [Traffic Policing: Example, page B-510](#)
- [Two-Rate Traffic Policing: Example, page B-510](#)
- [Multiple Traffic Policing Actions: Example, page B-511](#)
- [Explicit Congestion Notification: Example, page B-512](#)
- [Percentage-Based Policing and Shaping: Example, page B-513](#)
- [Bandwidth-Remaining Ratio: Example, page B-514](#)
- [Tunnel Marking: Example, page B-515](#)

**Traffic Policing: Example**

The following is sample output from the **show policy-map** command. This sample output displays the contents of a policy map called “policy1.” In policy 1, traffic policing on the basis of a committed information rate (CIR) of 20 percent has been configured, and the bc and be have been specified in milliseconds. As part of the traffic policing configuration, optional conform, exceed, and violate actions have been specified.

```
Router# show policy-map policy1

Policy Map policy1
Class class1
  police cir percent 20 bc 300 ms pir percent 40 be 400 ms
    conform-action transmit
    exceed-action drop
    violate-action drop
```

Table 39 describes the significant fields shown in the display.

**Table 39** *show policy-map Field Descriptions—Configured for Traffic Policing*

| Field      | Description                                                                                                                                                                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy Map | Name of policy map displayed.                                                                                                                                                                                                                                             |
| Class      | Name of the class configured in the policy map displayed.                                                                                                                                                                                                                 |
| police     | Indicates that traffic policing on the basis of specified percentage of bandwidth has been enabled. The committed burst (Bc) and excess burst (Be) sizes have been specified in milliseconds (ms), and optional conform, exceed, and violate actions have been specified. |

**Two-Rate Traffic Policing: Example**

The following is sample output from the **show policy-map** command when two-rate traffic policing has been configured. As shown below, two-rate traffic policing has been configured for a class called “police.” In turn, the class called police has been configured in a policy map called “policy1.” Two-rate traffic policing has been configured to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps.

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config-pmap-c)# interface serial3/0
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
```

The following sample output shows the contents of the policy map called “policy1”:

```
Router# show policy-map policy1

Policy Map policy1
Class police
  police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
  transmit exceed-action set-prec-transmit 2 violate-action drop
```

Traffic marked as conforming to the average committed rate (500 kbps) is sent as-is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, is marked with IP Precedence 2 and then sent. All traffic exceeding 1 Mbps is dropped. The burst parameters are set to 10000 bytes.

Table 40 describes the significant fields shown in the display.

**Table 40** *show policy-map Field Descriptions—Configured for Two-Rate Traffic Policing*

| Field          | Description                                                                                                                                                                                                                         |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| police         | Indicates that the <b>police</b> command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size (bc), peak information rate (PIR), and peak burst (BE) size used for marking packets. |
| conform-action | Displays the action to be taken on packets conforming to a specified rate.                                                                                                                                                          |
| exceed-action  | Displays the action to be taken on packets exceeding a specified rate.                                                                                                                                                              |
| violate-action | Displays the action to be taken on packets violating a specified rate.                                                                                                                                                              |

#### Multiple Traffic Policing Actions: Example

The following is sample output from the **show policy-map** command when the Policer Enhancement—Multiple Actions feature has been configured. The following sample output from the **show policy-map** command displays the configuration for a service policy called “police.” In this service policy, traffic policing has been configured to allow multiple actions for packets marked as conforming to, exceeding, or violating the CIR or the PIR shown in the example.

```
Router# show policy-map police

Policy Map police
Class class-default
  police cir 1000000 bc 31250 pir 2000000 be 31250
    conform-action transmit
    exceed-action set-prec-transmit 4
    exceed-action set-frde-transmit

    violate-action set-prec-transmit 2
    violate-action set-frde-transmit
```

Packets conforming to the specified CIR (1000000 bps) are marked as conforming packets. These are transmitted unaltered.

Packets exceeding the specified CIR (but not the specified PIR, 2000000 bps) are marked as exceeding packets. For these packets, the IP Precedence level is set to 4, the discard eligibility (DE) bit is set to 1, and the packet is transmitted.

Packets exceeding the specified PIR are marked as violating packets. For these packets, the IP Precedence level is set to 2, the DE bit is set to 1, and the packet is transmitted.



#### Note

Actions are specified by using the *action* argument of the **police** command. For more information about the available actions, see the **police** command reference page.

Table 41 describes the significant fields shown in the display.

**Table 41** *show policy-map Field Descriptions—Configured for Multiple Traffic Policing Actions*

| Field          | Description                                                                                                                                                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| police         | Indicates that the <b>police</b> command has been configured to enable traffic policing. Also, displays the specified CIR, BC, PIR, and BE used for marking packets. |
| conform-action | Displays the one or more actions to be taken on packets conforming to a specified rate.                                                                              |
| exceed-action  | Displays the one or more actions to be taken on packets exceeding a specified rate.                                                                                  |
| violate-action | Displays the one or more actions to be taken on packets violating a specified rate.                                                                                  |

#### Explicit Congestion Notification: Example

The following is sample output from the **show policy-map** command when the WRED—Explicit Congestion Notification (ECN) feature has been configured. The words “explicit congestion notification” (along with the ECN marking information) included in the output indicate that ECN has been enabled.

Router# **show policy-map**

```

Policy Map poll
  Class class-default
    Weighted Fair Queueing
      Bandwidth 70 (%)
      exponential weight 9
      explicit congestion notification
      class      min-threshold      max-threshold      mark-probability
      -----
      -----
      0          -                  -                  1/10
      1          -                  -                  1/10
      2          -                  -                  1/10
      3          -                  -                  1/10
      4          -                  -                  1/10
      5          -                  -                  1/10
      6          -                  -                  1/10
      7          -                  -                  1/10
      rsvp       -                  -                  1/10

```

Table 42 describes the significant fields shown in the display.

**Table 42** *show policy-map Field Descriptions—Configured for ECN*

| Field                            | Description                                                                           |
|----------------------------------|---------------------------------------------------------------------------------------|
| explicit congestion notification | Indication that Explicit Congestion Notification is enabled.                          |
| class                            | IP precedence value.                                                                  |
| min-threshold                    | Minimum threshold. Minimum WRED threshold in number of packets.                       |
| max-threshold                    | Maximum threshold. Maximum WRED threshold in number of packets.                       |
| mark-probability                 | Fraction of packets dropped when the average queue depth is at the maximum threshold. |

### Percentage-Based Policing and Shaping: Example

The following example displays the contents of two service policy maps—one called “policy1” and one called “policy2.” In policy1, traffic policing based on a CIR of 50 percent has been configured. In policy 2, traffic shaping based on an average rate of 35 percent has been configured.

```
Router# show policy-map policy1
```

```
Policy Map policy1
  class class1
    police cir percent 50
```

```
Router# show policy-map policy2
```

```
Policy Map policy2
  class class2
    shape average percent 35
```

The following example displays the contents of the service policy map called “po1”:

```
Router# show policy-map po1
```

```
Policy Map po1
  Weighted Fair Queueing
  Class class1
  Bandwidth 937 (kbps) Max thresh 64 (packets)
  Class class2
    Bandwidth 937 (kbps) Max thresh 64 (packets)
  Class class3
    Bandwidth 937 (kbps) Max thresh 64 (packets)
  Class class4
    Bandwidth 937 (kbps) Max thresh 64 (packets)
```

The following example displays the contents of all policy maps on the router:

```
Router# show policy-map
```

```
Policy Map poH1
  Weighted Fair Queueing
  Class class1
    Bandwidth 937 (kbps) Max thresh 64 (packets)
  Class class2
    Bandwidth 937 (kbps) Max thresh 64 (packets)
```

```

Class class3
  Bandwidth 937 (kbps)  Max thresh 64 (packets)
Class class4
  Bandwidth 937 (kbps)  Max thresh 64 (packets)
Policy Map policy2
  Weighted Fair Queueing
    Class class1
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class2
      Bandwidth 300 (kbps)  Max thresh 64 (packets)
    Class class3
      Bandwidth 300 (kbps)  Max thresh 64 (packets)
    Class class4
      Bandwidth 300 (kbps)  Max thresh 64 (packets)

```

Table 43 describes the significant fields shown in the display.

**Table 43** *show policy-map Field Descriptions—Configured for Percentage-Based Policing and Shaping*

| Field                  | Description                                                     |
|------------------------|-----------------------------------------------------------------|
| Policy Map             | Name of policy map displayed.                                   |
| Weighted Fair Queueing | Indicates that weighted fair queueing (WFQ) has been enabled.   |
| Class                  | Name of class configured in policy map displayed.               |
| Bandwidth              | Bandwidth, in kbps, configured for this class.                  |
| Max threshold          | Maximum threshold. Maximum WRED threshold in number of packets. |

#### Bandwidth-Remaining Ratio: Example

The following sample output for the **show policy-map** command indicates that the class-default class of the policy map named `vlan10_policy` has a bandwidth-remaining ratio of 10. When congestion occurs, the scheduler allocates class-default traffic 10 times the unused bandwidth allocated in relation to other subinterfaces.

Router# **show policy-map vlan10\_policy**

```

Policy Map vlan10_policy
  Class class-default
    Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 10
      service-policy child_policy

```

Table 44 describes the fields shown in the display.

**Table 44** *show policy-map Field Descriptions—Configured for Bandwidth-Remaining Ratio*

| Field                        | Description                                                |
|------------------------------|------------------------------------------------------------|
| Policy Map                   | Name of the policy map being displayed.                    |
| Class                        | Name of the class in the policy map being displayed.       |
| Average Rate Traffic Shaping | Indicates that Average Rate Traffic Shaping is configured. |
| cir                          | Committed information rate (CIR) used to shape traffic.    |
| bandwidth remaining ratio    | Indicates the ratio used to allocate excess bandwidth.     |

**Tunnel Marking: Example**

In this sample output of the **show policy-map** command, the character string “ip precedence tunnel 4” indicates that tunnel marking (either L2TPv3 or GRE) has been configured to set the IP precedence value to 4 in the header of a tunneled packet.

```
Router# show policy-map

Policy Map TUNNEL_MARKING
  Class MATCH_FRDE
    set ip precedence tunnel 4
```

Table 45 describes the fields shown in the display.

**Table 45** *show policy-map Field Descriptions—Configured for Tunnel Marking*

| Field                    | Description                                          |
|--------------------------|------------------------------------------------------|
| Policy Map               | Name of the policy map being displayed.              |
| Class                    | Name of the class in the policy map being displayed. |
| set ip precedence tunnel | Indicates that tunnel marking has been configured.   |

**Related Commands**

| Command                          | Description                                                                                                                                                                         |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bandwidth</b>                 | Specifies or modifies the bandwidth allocated for a class belonging to a policy map, and enables ATM overhead accounting.                                                           |
| <b>class (policy map)</b>        | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.       |
| <b>class-map</b>                 | Creates a class map to be used for matching packets to a specified class.                                                                                                           |
| <b>drop</b>                      | Configures a traffic class to discard packets belonging to a specific class.                                                                                                        |
| <b>police</b>                    | Configures traffic policing.                                                                                                                                                        |
| <b>police (two rates)</b>        | Configures traffic policing using two rates, the CIR and the PIR.                                                                                                                   |
| <b>policy-map</b>                | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                        |
| <b>shape</b>                     | Shapes traffic to the indicated bit rate according to the algorithm specified, and enables ATM overhead accounting.                                                                 |
| <b>show policy-map class</b>     | Displays the configuration for the specified class of the specified policy map.                                                                                                     |
| <b>show policy-map interface</b> | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |
| <b>show running-config</b>       | Displays the current configuration of the router. If configured, the command output includes information about ATM overhead accounting.                                             |
| <b>show table-map</b>            | Displays the configuration of a specified table map or of all table maps.                                                                                                           |
| <b>table-map (value mapping)</b> | Creates and configures a mapping table for mapping and converting one packet-marking value to another.                                                                              |

# show policy-map interface

To display the statistics and the configurations of the input and output policies that are attached to an interface, use the **show policy-map interface** command in user EXEC or privileged EXEC mode.

**show policy-map interface** [**type access-control**] *type number* [**vc** [*vpi/*] *vci*] [**dlci** *dlci*]  
[**input** | **output**]

| Syntax Description         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>type access-control</b> | (Optional) Displays class maps configured to determine the exact pattern to look for in the protocol stack of interest.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <i>type</i>                | Interface or subinterface whose policy configuration is to be displayed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <i>number</i>              | Port, connector, or interface card number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>vc</b>                  | (Optional) Specifies the policy configuration for a PVC; applies to ATM interfaces only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <i>vpi/</i>                | <p>(Optional) ATM network virtual path identifier (VPI) for this permanent virtual circuit (PVC). On the Cisco 7200 and 7500 series routers, this value ranges from 0 to 255.</p> <p>The <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.</p> <p>The absence of both the forward slash (/) and a <i>vpi</i> value defaults the <i>vpi</i> value to 0. If this value is omitted, information for all virtual circuits (VCs) on the specified ATM interface or subinterface is displayed.</p>                                                                                                                                                                                                                  |
| <i>vci</i>                 | <p>(Optional) ATM network virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the <b>atm vc-per-vp</b> command. Typically, the lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance [OAM], switched virtual circuit [SVC] signaling, Integrated Local Management Interface [ILMI], and so on) and should not be used.</p> <p>The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only.</p> <p>The <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.</p> |
| <b>dlci</b>                | (Optional) Indicates a specific PVC for which policy configuration is displayed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <i>dlci</i>                | (Optional) A specific data-link connection identifier (DLCI) number used on the interface. Policy configuration for the corresponding PVC is displayed when a DLCI is specified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>input</b>               | (Optional) Indicates that the statistics for the attached input policy are displayed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>output</b>              | (Optional) Indicates that the statistics for the attached output policy are displayed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Command Default

This command displays the packet statistics of all classes that are configured for all service policies on the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface.



The absence of both the forward slash (/) and a *vpi* value defaults the *vpi* value to 0. If this value is omitted, information for all virtual circuits (VCs) on the specified ATM interface or subinterface is displayed.

## Command Modes

Privileged EXEC (#)

### ATM Shared Port Adapter

User EXEC (>)

Privileged EXEC (#)

## Command History

| Release   | Modification                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(5)T  | This command was introduced.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE.                                                                                                                                                                                                                                                                                                                                                                                                            |
| 12.0(7)S  | This command was integrated into Cisco IOS Release 12.0(7)S.                                                                                                                                                                                                                                                                                                                                                                                                             |
| 12.0(28)S | This command was modified for the QoS: Percentage-Based Policing feature to include milliseconds when calculating the committed (conform) burst (bc) and excess (peak) burst (be) sizes.                                                                                                                                                                                                                                                                                 |
| 12.1(1)E  | This command was integrated into Cisco IOS Release 12.1(1)E.                                                                                                                                                                                                                                                                                                                                                                                                             |
| 12.1(2)T  | This command was modified to display information about the policy for all Frame Relay PVCs on the interface or, if a DLCI is specified, the policy for that specific PVC. This command was also modified to display the total number of packets marked by the quality of service (QoS) set action.                                                                                                                                                                       |
| 12.1(3)T  | This command was modified to display per-class accounting statistics.                                                                                                                                                                                                                                                                                                                                                                                                    |
| 12.2(4)T  | This command was modified for two-rate traffic policing and can display burst parameters and associated actions.                                                                                                                                                                                                                                                                                                                                                         |
| 12.2(8)T  | <p>The command was modified for the Policer Enhancement—Multiple Actions feature and the WRED—Explicit Congestion Notification (ECN) feature.</p> <p>For the Policer Enhancement—Multiple Actions feature, the command was modified to display the multiple actions configured for packets conforming to, exceeding, or violating a specific rate.</p> <p>For the WRED—Explicit Congestion Notification (ECN) feature, the command displays ECN marking information.</p> |

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(28)S | This command was modified for the QoS: Percentage-Based Policing feature to include milliseconds when calculating the committed (conform) burst (bc) and excess (peak) burst (be) sizes.                                                                                                                                                                                                                                                                                 |
| 12.1(1)E  | This command was integrated into Cisco IOS Release 12.1(1)E.                                                                                                                                                                                                                                                                                                                                                                                                             |
| 12.1(2)T  | This command was modified to display information about the policy for all Frame Relay PVCs on the interface or, if a DLCI is specified, the policy for that specific PVC. This command was also modified to display the total number of packets marked by the quality of service (QoS) set action.                                                                                                                                                                       |
| 12.1(3)T  | This command was modified to display per-class accounting statistics.                                                                                                                                                                                                                                                                                                                                                                                                    |
| 12.2(4)T  | This command was modified for two-rate traffic policing and can display burst parameters and associated actions.                                                                                                                                                                                                                                                                                                                                                         |
| 12.2(8)T  | <p>The command was modified for the Policer Enhancement—Multiple Actions feature and the WRED—Explicit Congestion Notification (ECN) feature.</p> <p>For the Policer Enhancement—Multiple Actions feature, the command was modified to display the multiple actions configured for packets conforming to, exceeding, or violating a specific rate.</p> <p>For the WRED—Explicit Congestion Notification (ECN) feature, the command displays ECN marking information.</p> |

| Release          | Modification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.4(4)T         | The <b>type access-control</b> keywords were added to support flexible packet matching.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 12.2(28)SB       | This command was integrated into Cisco IOS Release 12.2(28)SB, and the following modifications were made: <ul style="list-style-type: none"> <li>This command was modified to display either legacy (undistributed processing) QoS or hierarchical queueing framework (HQF) parameters on Frame Relay interfaces or PVCs.</li> <li>This command was modified to display information about Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunnel marking.</li> </ul>                                                                                                                                                     |
| 12.2(31)SB2      | The following modifications were made: <ul style="list-style-type: none"> <li>This command was enhanced to display statistical information for each level of priority service configured and information about bandwidth-remaining ratios, and this command was implemented on the Cisco 10000 series router for the PRE3.</li> <li>This command was modified to display statistics for matching packets on the basis of VLAN identification numbers. As of Cisco IOS Release 12.2(31)SB2, matching packets on the basis of VLAN identification numbers is supported on Cisco 10000 series routers only.</li> </ul> |
| 12.2(33)SRC      | This command was integrated into Cisco IOS Release 12.2(33)SRC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 12.4(15)T2       | This command was modified to display information about Generic Routing Encapsulation (GRE) tunnel marking. <p><b>Note</b> As of this release, GRE-tunnel marking is supported on the Cisco MGX Route Processor Module (RPM-XF) platform <i>only</i>.</p>                                                                                                                                                                                                                                                                                                                                                            |
| 12.2(33)SB       | This command was modified to display information about GRE-tunnel marking, and support for the Cisco 7300 series router was added.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Cisco IOS XE 2.1 | This command was integrated into Cisco IOS XE Release 2.1 and was implemented on the Cisco ASR 1000 series router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 12.4(20)T        | Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 12.2(33)SXI      | This command was implemented on the Catalyst 6500 series switch and modified to display the strict level in the priority feature and the counts per level.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 12.4(20)MR       | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 12.2(33)MRA      | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

### Usage Guidelines

The **show policy-map interface** command displays the packet statistics for classes on the specified interface or the specified PVC only if a service policy has been attached to the interface or the PVC. The counters displayed after the **show policy-map interface** command is entered are updated only if congestion is present on the interface.

### Examples

This section provides sample output from typical **show policy-map interface** commands. Depending upon the interface or platform in use and the options enabled, the output you see may vary slightly from the ones shown below.

- [Traffic Shaping on Serial Interface: Example, page B-520](#)
- [Two-Rate Traffic Policing: Example, page B-523](#)
- [Multiple Traffic Policing Actions: Example, page B-524](#)
- [Percentage-Based Policing and Shaping: Example, page B-526](#)
- [Traffic Shaping: Example, page B-527](#)
- [Traffic Policing: Example, page B-529](#)

### Traffic Shaping on Serial Interface: Example

The following sample output from the **show policy-map interface** command displays the statistics for the serial 3/2 interface, to which a service policy called p1 (configured as shown below) is attached. Traffic shaping has been enabled on this interface. See [Table 46](#) for an explanation of the significant fields that commonly appear in the command output.

```
policy-map p1
  class c1
    shape average 320000
```

```
Router# show policy-map interface serial3/2 output
```

```
Serial3/2
```

```
Service-policy output: p1
```

```
Class-map: c1 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: ip precedence 0
  Traffic Shaping
    Target    Byte    Sustain  Excess   Interval  Increment Adapt
    Rate      Limit  bits/int bits/int (ms)      (bytes)  Active
    320000    2000   8000     8000     25        1000     -

    Queue     Packets  Bytes    Packets  Bytes    Shaping
    Depth                                Delayed  Delayed  Active
    0          0         0         0         0         no
```

```

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match: any

```

Table 46 describes significant fields commonly shown in the displays. The fields in the table are grouped according to the relevant QoS feature.

**Table 46** *show policy-map interface Field Descriptions<sup>1</sup>*

| Field                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Fields Associated with Classes or Service Policies</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Service-policy output                                     | Name of the output service policy applied to the specified interface or VC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Class-map                                                 | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| packets and bytes                                         | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| offered rate                                              | Rate, in kbps, of packets coming in to the class.<br><br><b>Note</b> If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified <i>before</i> they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only <i>one</i> tunnel encapsulation, or may include the overhead for <i>all</i> tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| drop rate                                                 | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Note</b>                                               | In distributed architecture platforms (such as the Cisco 7500 series platform), the value of the transfer rate, calculated as the difference between the offered rate and the drop rate counters, can sporadically deviate from the average by up to 20 percent or more. This can occur while no corresponding burst is registered by independent traffic analyzer equipment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Match                                                     | Match criteria specified for the class of traffic. Choices include criteria such as IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental (EXP) value, access groups, and QoS groups. For more information about the variety of match criteria that are available, see the “Classifying Network Traffic” module in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .                                                                                                                                                                                                                                                                                                                                                                                                                |

**Table 46** *show policy-map interface Field Descriptions<sup>1</sup> (continued)*

| Field                                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Fields Associated with Queueing (if Enabled)</b>                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Output Queue                                                                      | The weighted fair queueing (WFQ) conversation to which this class of traffic is allocated.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Bandwidth                                                                         | Bandwidth, in either kbps or percentage, configured for this class and the burst size.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| pkts matched/bytes matched                                                        | Number of packets (also shown in bytes) matching this class that were placed in the queue. This number reflects the total number of matching packets queued at any time. Packets matching this class are queued only when congestion exists. If packets match the class but are never queued because the network was not congested, those packets are not included in this total. However, if process switching is in use, the number of packets is always incremented even if the network is not congested. |
| depth/total drops/no-buffer drops                                                 | Number of packets discarded for this class. No-buffer indicates that no memory buffer exists to service the packet.                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Fields Associated with Weighted Random Early Detection (WRED) (if Enabled)</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| exponential weight                                                                | Exponent used in the average queue size calculation for a WRED parameter group.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| mean queue depth                                                                  | Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a fluctuating average. The minimum and maximum thresholds are compared against this value to determine drop decisions.                                                                                                                                                                                                                                                                    |
| class                                                                             | IP precedence level.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Transmitted pkts/bytes                                                            | <p>Number of packets (also shown in bytes) passed through WRED and not dropped by WRED.</p> <p><b>Note</b> If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped <i>after</i> the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as “no-buffer drops”) are not taken into account by the WRED packet counter.</p>                                                                              |
| Random drop pkts/bytes                                                            | Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level.                                                                                                                                                                                                                                                                                                             |
| Tail drop pkts/bytes                                                              | Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level.                                                                                                                                                                                                                                                                                                                                                                       |
| Minimum thresh                                                                    | Minimum threshold. Minimum WRED threshold in number of packets.                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Maximum thresh                                                                    | Maximum threshold. Maximum WRED threshold in number of packets.                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Mark prob                                                                         | Mark probability. Fraction of packets dropped when the average queue depth is at the maximum threshold.                                                                                                                                                                                                                                                                                                                                                                                                      |

**Table 46** *show policy-map interface Field Descriptions<sup>1</sup> (continued)*

| Field                                                      | Description                                                                                                                                                                             |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Fields Associated with Traffic Shaping (if Enabled)</b> |                                                                                                                                                                                         |
| Target Rate                                                | Rate used for shaping traffic.                                                                                                                                                          |
| Byte Limit                                                 | Maximum number of bytes that can be transmitted per interval. Calculated as follows:<br>$((Bc+Be) / 8) \times 1$                                                                        |
| Sustain bits/int                                           | Committed burst (Bc) rate.                                                                                                                                                              |
| Excess bits/int                                            | Excess burst (Be) rate.                                                                                                                                                                 |
| Interval (ms)                                              | Time interval value in milliseconds (ms).                                                                                                                                               |
| Increment (bytes)                                          | Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval.                                                                              |
| Queue Depth                                                | Current queue depth of the traffic shaper.                                                                                                                                              |
| Packets                                                    | Total number of packets that have entered the traffic shaper system.                                                                                                                    |
| Bytes                                                      | Total number of bytes that have entered the traffic shaper system.                                                                                                                      |
| Packets Delayed                                            | Total number of packets delayed in the queue of the traffic shaper before being transmitted.                                                                                            |
| Bytes Delayed                                              | Total number of bytes delayed in the queue of the traffic shaper before being transmitted.                                                                                              |
| Shaping Active                                             | Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a “yes” appears in this field. |

1. A number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

### Two-Rate Traffic Policing: Example

The following is sample output from the **show policy-map interface** command when two-rate traffic policing has been configured. In the example below, 1.25 Mbps of traffic is sent (“offered”) to a policer class.

Router# **show policy-map interface serial3/0**

Serial3/0

Service-policy output: policy1

```

Class-map: police (match all)
  148803 packets, 36605538 bytes
  30 second offered rate 1249000 bps, drop rate 249000 bps
  Match: access-group 101
  police:
    cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
    conformed 59538 packets, 14646348 bytes; action: transmit
    exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
    violated 29731 packets, 7313826 bytes; action: drop
    conformed 499000 bps, exceed 500000 bps violate 249000 bps
Class-map: class-default (match-any)
  19 packets, 1990 bytes
  30 seconds offered rate 0 bps, drop rate 0 bps
  Match: any

```

The two-rate traffic policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming are sent as is, and packets marked as exceeding are marked with IP Precedence 2 and then sent. Packets marked as violating the specified rate are dropped.

Table 47 describes the significant fields shown in the display.

**Table 47** *show policy-map interface Field Descriptions—Configured for Two-Rate Traffic Policing*

| Field     | Description                                                                                                                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| police    | Indicates that the <b>police</b> command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size, peak information rate (PIR), and peak burst size used for marking packets. |
| conformed | Displays the action to be taken on packets conforming to a specified rate. Displays the number of packets and bytes on which the action was taken.                                                                        |
| exceeded  | Displays the action to be taken on packets exceeding a specified rate. Displays the number of packets and bytes on which the action was taken.                                                                            |
| violated  | Displays the action to be taken on packets violating a specified rate. Displays the number of packets and bytes on which the action was taken.                                                                            |

#### Multiple Traffic Policing Actions: Example

The following is sample output from the **show policy-map** command when the Policer Enhancement—Multiple Actions feature has been configured. The sample output from the **show policy-map interface** command displays the statistics for the serial 3/2 interface, to which a service policy called “police” (configured as shown below) is attached.

```
policy-map police
  class class-default
    police cir 1000000 pir 2000000
      conform-action transmit
      exceed-action set-prec-transmit 4
      exceed-action set-frde-transmit
      violate-action set-prec-transmit 2
      violate-action set-frde-transmit
```

```
Router# show policy-map interface serial3/2
```

```
Serial3/2: DLCI 100 -
```

```
Service-policy output: police
```

```
Class-map: class-default (match-any)
  172984 packets, 42553700 bytes
  5 minute offered rate 960000 bps, drop rate 277000 bps
  Match: any
  police:
    cir 1000000 bps, bc 31250 bytes, pir 2000000 bps, be 31250 bytes
    conformed 59679 packets, 14680670 bytes; actions:
      transmit
  exceeded 59549 packets, 14649054 bytes; actions:
    set-prec-transmit 4
    set-frde-transmit
  violated 53758 packets, 13224468 bytes; actions:
    set-prec-transmit 2
    set-frde-transmit
  conformed 340000 bps, exceed 341000 bps, violate 314000 bps
```



The sample output from **show policy-map interface** command shows the following:

- 59679 packets were marked as conforming packets (that is, packets conforming to the CIR) and were transmitted unaltered.
- 59549 packets were marked as exceeding packets (that is, packets exceeding the CIR but not exceeding the PIR). Therefore, the IP Precedence value of these packets was changed to an IP Precedence level of 4, the discard eligibility (DE) bit was set to 1, and the packets were transmitted with these changes.
- 53758 packets were marked as violating packets (that is, exceeding the PIR). Therefore, the IP Precedence value of these packets was changed to an IP Precedence level of 2, the DE bit was set to 1, and the packets were transmitted with these changes.


**Note**

Actions are specified by using the *action* argument of the **police** command. For more information about the available actions, see the **police** command reference page.

Table 48 describes the significant fields shown in the display.

**Table 48** *show policy-map interface Field Descriptions—Configured for Multiple Traffic Policing Actions*

| Field                              | Description                                                                                                                                                                                                 |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| police                             | Indicates that the <b>police</b> command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size (BC), PIR, and peak burst size (BE) used for marking packets. |
| conformed, packets, bytes, actions | Displays the number of packets (also shown in bytes) marked as conforming to a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately.         |
| exceeded, packets, bytes, actions  | Displays the number of packets (also shown in bytes) marked as exceeding a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately.             |
| violated, packets, bytes, actions  | Displays the number of packets (also shown in bytes) marked as violating a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately.             |

**Percentage-Based Policing and Shaping: Example**

The following sample output from the **show policy-map interface** command shows traffic policing configured using a CIR based on a bandwidth of 20 percent. The CIR and committed burst (Bc) in milliseconds (ms) are included in the display.

```
Router# show policy-map interface Serial3/1

Serial3/1

Service-policy output: mypolicy

Class-map: gold (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
  police:
    cir 20 % bc 10 ms
    cir 2000000 bps, bc 2500 bytes
    pir 40 % be 20 ms
    pir 4000000 bps, be 10000 bytes
  conformed 0 packets, 0 bytes; actions:
    transmit
  exceeded 0 packets, 0 bytes; actions:
    drop
  violated 0 packets, 0 bytes; actions:
    drop
  conformed 0 bps, exceed 0 bps, violate 0 bps
```

Table 49 describes the significant fields shown in the display.

**Table 49** *show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping<sup>1</sup>*

| Field                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service-policy output | Name of the output service policy applied to the specified interface or VC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Class-map             | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| packets, bytes        | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| offered rate          | <p>Rate, in kbps, of packets coming in to the class.</p> <p><b>Note</b> If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified <i>before</i> they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only <i>one</i> tunnel encapsulation, or may include the overhead for <i>all</i> tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.</p> |

**Table 49** *show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping<sup>1</sup>*

| Field              | Description                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| police             | Indicates that traffic policing based on a percentage of bandwidth has been enabled. Also, displays the bandwidth percentage, the CIR, and the committed burst (Bc) size in ms. |
| conformed, actions | Displays the number of packets and bytes marked as conforming to the specified rates, and the action to be taken on those packets.                                              |
| exceeded, actions  | Displays the number of packets and bytes marked as exceeding the specified rates, and the action to be taken on those packets.                                                  |

1. A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

### Traffic Shaping: Example

The following sample output from the **show policy-map interface** command (shown below) displays the statistics for the serial 3/2 interface. Traffic shaping has been enabled on this interface, and an average rate of 20 percent of the bandwidth has been specified.

Router# **show policy-map interface Serial3/2**

Serial3/2

Service-policy output: p1

Class-map: c1 (match-all)

0 packets, 0 bytes

5 minute offered rate 0 bps, drop rate 0 bps

Match: any

Traffic Shaping

| Target/Average<br>Rate | Byte<br>Limit | Sustain<br>bits/int | Excess<br>bits/int | Interval<br>(ms) | Increment<br>(bytes) | Adapt<br>Active |
|------------------------|---------------|---------------------|--------------------|------------------|----------------------|-----------------|
| 20 %                   |               | 10 (ms)             | 20 (ms)            |                  |                      |                 |
| 201500/201500          | 1952          | 7808                | 7808               | 38               | 976                  | -               |

| Queue<br>Depth | Packets | Bytes | Packets<br>Delayed | Bytes<br>Delayed | Shaping<br>Active |
|----------------|---------|-------|--------------------|------------------|-------------------|
| 0              | 0       | 0     | 0                  | 0                | no                |

Table 50 describes the significant fields shown in the display.

**Table 50** *show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping (with Traffic Shaping Enabled)<sup>1</sup>*

| Field                 | Description                                                                                                                                                                                                               |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service-policy output | Name of the output service policy applied to the specified interface or VC.                                                                                                                                               |
| Class-map             | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes        | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.                                                                                                                  |

**Table 50** *show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping (with Traffic Shaping Enabled)<sup>1</sup> (continued)*

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| offered rate        | Rate, in kbps, of packets coming in to the class.<br><br><b>Note</b> If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified <i>before</i> they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only <i>one</i> tunnel encapsulation, or may include the overhead for <i>all</i> tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| drop rate           | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Match               | Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and quality of service (QoS) groups. For more information about the variety of match criteria that are available, see the “Classifying Network Traffic” module in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Traffic Shaping     | Indicates that traffic shaping based on a percentage of bandwidth has been enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Target/Average Rate | Rate (percentage) used for shaping traffic and the number of packets meeting that rate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Byte Limit          | Maximum number of bytes that can be transmitted per interval. Calculated as follows:<br>$((Bc+Be) / 8 ) \times 1$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Sustain bits/int    | Committed burst (Bc) rate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Excess bits/int     | Excess burst (Be) rate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Interval (ms)       | Time interval value in milliseconds (ms).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Increment (bytes)   | Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Adapt Active        | Indicates whether adaptive shaping is enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Queue Depth         | Current queue depth of the traffic shaper.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Packets             | Total number of packets that have entered the traffic shaper system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Bytes               | Total number of bytes that have entered the traffic shaper system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

**Table 50** *show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping (with Traffic Shaping Enabled)<sup>1</sup> (continued)*

| Field           | Description                                                                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Packets Delayed | Total number of packets delayed in the queue of the traffic shaper before being transmitted.                                                                                            |
| Bytes Delayed   | Total number of bytes delayed in the queue of the traffic shaper before being transmitted.                                                                                              |
| Shaping Active  | Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a “yes” appears in this field. |

1. A number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

### Traffic Policing: Example

The following is sample output from the **show policy-map interface** command. This sample displays the statistics for the serial 2/0 interface on which traffic policing has been enabled. The committed (conform) burst (bc) and excess (peak) burst (be) are specified in milliseconds (ms).

```
Router# show policy-map interface serial2/0

Serial2/0

Service-policy output: policy1 (1050)

Class-map: class1 (match-all) (1051/1)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: ip precedence 0 (1052)
  police:
    cir 20 % bc 300 ms
    cir 409500 bps, bc 15360 bytes
    pir 40 % be 400 ms
    pir 819000 bps, be 40960 bytes
    conformed 0 packets, 0 bytes; actions:
      transmit
    exceeded 0 packets, 0 bytes; actions:
      drop
    violated 0 packets, 0 bytes; actions:
      drop
    conformed 0 bps, exceed 0 bps, violate 0 bps

Class-map: class-default (match-any) (1054/0)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any (1055)
    0 packets, 0 bytes
    5 minute rate 0 bps
```

In this example, the CIR and PIR are displayed in bps, and both the committed burst (bc) and excess burst (be) are displayed in bits.

The CIR, PIR bc, and be are calculated on the basis of the formulas described below.

**Formula for Calculating the CIR: Example**

When calculating the CIR, the following formula is used:

- CIR percentage specified (as shown in the output from the **show policy-map** command) \* bandwidth (BW) of the interface (as shown in the output from the **show interfaces** command) = total bits per second

According to the output from the **show interfaces** command for the serial 2/0 interface, the interface has a bandwidth (BW) of 2048 kbps.

```
Router# show interfaces serial2/0
```

```
Serial2/0 is administratively down, line protocol is down
Hardware is M4T
MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the CIR:

$$20 \% * 2048 \text{ kbps} = 409600 \text{ bps}$$

**Formula for Calculating the PIR: Example**

When calculating the PIR, the following formula is used:

- PIR percentage specified (as shown in the output from the **show policy-map** command) \* bandwidth (BW) of the interface (as shown in the output from the **show interfaces** command) = total bits per second

According to the output from the **show interfaces** command for the serial 2/0 interface, the interface has a bandwidth (BW) of 2048 kbps.

```
Router# show interfaces serial2/0
```

```
Serial2/0 is administratively down, line protocol is down
Hardware is M4T
MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the PIR:

$$40 \% * 2048 \text{ kbps} = 819200 \text{ bps}$$




---

**Note** Discrepancies between this total and the total shown in the output from the **show policy-map interface** command can be attributed to a rounding calculation or to differences associated with the specific interface configuration.

---

**Formula for Calculating the Committed Burst (bc): Example**

When calculating the bc, the following formula is used:

- The bc in milliseconds (as shown in the **show policy-map** command) \* the CIR in bits per seconds = total number bytes

The following values are used for calculating the bc:

$$300 \text{ ms} * 409600 \text{ bps} = 15360 \text{ bytes}$$

**Formula for Calculating the Excess Burst (be): Example**

When calculating the bc and the be, the following formula is used:

- The be in milliseconds (as shown in the **show policy-map** command) \* the PIR in bits per seconds = total number bytes

The following values are used for calculating the be:

$$400 \text{ ms} * 819200 \text{ bps} = 40960 \text{ bytes}$$

Table 51 describes the significant fields shown in the display.

**Table 51** show policy-map interface Field Descriptions

| Field                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service-policy output | Name of the output service policy applied to the specified interface or VC.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Class-map             | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.                                                                                                                                                                                                                                                                           |
| packets and bytes     | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.                                                                                                                                                                                                                                                                                                                                                                                            |
| offered rate          | Rate, in kbps, of packets coming in to the class.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| drop rate             | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.                                                                                                                                                                                                                                                                                                                        |
| Match                 | Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) groups. For more information about the variety of match criteria that are available, see the “Classifying Network Traffic” module in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> . |
| police                | Indicates that traffic policing has been enabled. Display includes the CIR, PIR (in both a percentage of bandwidth and in bps) and the bc and be in bytes and milliseconds. Also displays the optional conform, exceed, and violate actions, if any, and the statistics associated with these optional actions.                                                                                                                                                                                     |

#### Related Commands

| Command                                | Description                                                                                                                                                                           |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bandwidth remaining ratio</b>       | Specifies a bandwidth-remaining ratio for class queues and subinterface-level queues to determine the amount of unused (excess) bandwidth to allocate to the queue during congestion. |
| <b>class-map</b>                       | Creates a class map to be used for matching packets to a specified class.                                                                                                             |
| <b>compression header ip</b>           | Configures RTP or TCP IP header compression for a specific class.                                                                                                                     |
| <b>drop</b>                            | Configures a traffic class to discard packets belonging to a specific class.                                                                                                          |
| <b>match packet length (class-map)</b> | Specifies the length of the Layer 3 packet in the IP header as a match criterion in a class map.                                                                                      |
| <b>police</b>                          | Configures traffic policing.                                                                                                                                                          |
| <b>police (percent)</b>                | Configures traffic policing on the basis of a percentage of bandwidth available on an interface.                                                                                      |
| <b>police (two rates)</b>              | Configures traffic policing using two rates, the CIR and the PIR.                                                                                                                     |
| <b>policy-map</b>                      | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                          |
| <b>priority</b>                        | Specifies that low-latency behavior must be given to a traffic class and configures multiple priority queues.                                                                         |

| Command                      | Description                                                                                                               |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>random-detect ecn</b>     | Enables ECN.                                                                                                              |
| <b>shape (percent)</b>       | Specifies average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface.       |
| <b>show class-map</b>        | Display all class maps and their matching criteria.                                                                       |
| <b>show interfaces</b>       | Displays statistics for all interfaces configured on a router or access server.                                           |
| <b>show mls qos</b>          | Displays MLS QoS information.                                                                                             |
| <b>show policy-map</b>       | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| <b>show policy-map class</b> | Displays the configuration for the specified class of the specified policy map.                                           |



# show ppp multilink

To display bundle information for Multilink PPP (MLP) bundles, use the **show ppp multilink** command in privileged EXEC mode.

**show ppp multilink** [**active** | **inactive** | **interface** *bundle-interface* | [**username** *name*] [**endpoint** *discriminator*]]

| Syntax Description                       |            |                                                                                                |
|------------------------------------------|------------|------------------------------------------------------------------------------------------------|
| <b>active</b>                            | (Optional) | Displays information about active multilink bundles only.                                      |
| <b>inactive</b>                          | (Optional) | Displays information about inactive multilink bundles only.                                    |
| <b>interface</b> <i>bundle-interface</i> | (Optional) | Displays information for the specified bundle interface.                                       |
| <b>username</b> <i>name</i>              | (Optional) | Displays information for all multilink bundles that have the specified peer username.          |
| <b>endpoint</b> <i>discriminator</i>     | (Optional) | Displays information for all multilink bundles that have the specified endpoint discriminator. |

**Command Modes** Privileged EXEC

| Command History | Release     | Modification                                                                                                                                                   |
|-----------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.4(19)MR1 | This command was integrated into Cisco IOS Release 12.4(19)MR1.                                                                                                |
|                 | 12.4(20)MR  | This command was modified for the dIPHC and dMLPPP offload features. The command output differs for MLPPP bundles that are offloaded to the network processor. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. Release 12.2(33)MRA does not support dIPHC.                                                    |

**Examples** The following is sample output from the **show ppp multilink** command when no bundles are on a system:

```
Router# show ppp multilink
```

```
No active bundles
```

The following sample output is for a single bundle that is offloaded to the network processor.

```
Router# show ppp multilink
```

```
Multilink1
  Bundle name: pas1_1
  Remote Endpoint Discriminator: [1] pas1_1
  Local Endpoint Discriminator: [1] pas3_1
  Bundle up for 22:58:45, total bandwidth 7936, load 1/255
  Receive buffer limit 48000 bytes, frag timeout 1000 ms
  Distributed MLP bundle status is: tx_active rx_active
    last rx seq no: 0x3E3998
      rx frames:      3
      rx iw frames:   129369198
```

# show ppp multilink

```

rx err mrru:      0
rx err iw mru:    0
rx err iw fbp:    0
rx flushed:       0
last tx seq no:   0x4
tx frames:        4
tx err mrru:      0

```

```

Member links: 4 active, 0 inactive (max not set, min not set)
Se0/0:0, since 22:58:46, 7440 weight, 42 frag size, ACT rx link seq: 0x3E399C
Se0/1:0, since 22:58:46, 7440 weight, 42 frag size, ACT x link seq: 0x3E3997
Se0/2:0, since 22:58:45, 7440 weight, 42 frag size, ACT rx link seq: 0x3E3995
Se0/3:0, since 22:58:45, 7440 weight, 42 frag size, ACT rx link seq: 0x3E3996

```

The following is another example of sample output when a single MLP bundle (named 7206-3) is on a system and is not offloaded to the network processor:

Router# **show ppp multilink**

```

Virtual-Access4
Bundle name: 7206-3
Remote Endpoint Discriminator: [1] 7206-3
Local Endpoint Discriminator: [1] 7206-4
Bundle up for 00:00:07, total bandwidth 64, load 1/255
Receive buffer limit 12192 bytes, frag timeout 1000 ms
0/0 fragments/bytes in reassembly list
0 lost fragments, 0 reordered
0/0 discarded fragments/bytes, 0 lost received
0x0 received sequence, 0x0 sent sequence
Member links: 1 active, 0 inactive (max not set, min not set)
BR2/0:1, since 01:59:35, 80 weight, 72 frag size

```

# show ptp clock

Displays information about the PTP clock.

**show ptp clock**

|                           |                                            |
|---------------------------|--------------------------------------------|
| <b>Syntax Description</b> | This command has no arguments or keywords. |
|---------------------------|--------------------------------------------|

|                      |           |
|----------------------|-----------|
| <b>Command Modes</b> | User EXEC |
|----------------------|-----------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(12)MR2 | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |
|                 |             |                                                                 |

|                         |                                                                                   |
|-------------------------|-----------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | Use the <b>show ptp clock</b> command to display information about the PTP clock. |
|-------------------------|-----------------------------------------------------------------------------------|

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | <pre>Router# show ptp clock PTP CLOCK INFO   PTP Device Type: Ordinary clock   Clock Identity: 0x0:1E:4A:FF:FF:96:A9:9E   Clock Domain: 2   Number of PTP ports: 1   Priority1: 128   Priority2: 128   Clock Quality:     Class: 13     Accuracy: Within 1s     Offset (log variance): 52592   Offset From Master: 0   Mean Path Delay: 0   Steps Removed: 0   Local clock time: 19:58:40 UTC Oct 30 2000</pre> |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| Related Commands | Command                               | Description                                    |
|------------------|---------------------------------------|------------------------------------------------|
|                  | <b>show ptp foreign-master-record</b> | Displays the PTP foreign master records.       |
|                  | <b>show ptp parent</b>                | Displays the PTP parent properties.            |
|                  | <b>show ptp port</b>                  | Displays the PTP port properties.              |
|                  | <b>show ptp time-property</b>         | Displays the time properties of the PTP clock. |

# show ptp foreign-master-record

To display the PTP foreign master record set, use the **show ptp foreign-master-record** command in user EXEC mode.

**show ptp foreign-master-record**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(12)MR2 | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** Use the **show ptp foreign-master-record** command to display the PTP foreign master records.

**Examples** The following example shows output from the **show ptp foreign-master-record** command:

```
Router# show ptp foreign-master-record
PTP FOREIGN MASTER RECORDS
Interface Vlan2
Number of foreign records 1, max foreign records 5
Best foreign record 0
RECORD #0
Foreign master port identity: clock id: 0x0:1E:4A:FF:FF:96:D2:A9
Foreign master port identity: port num: 1
Number of Announce messages: 8
Number of Current Announce messages: 6
Time stamps: 1233935406, 664274927
```

| Related Commands | Command                       | Description                                    |
|------------------|-------------------------------|------------------------------------------------|
|                  | <b>show ptp clock</b>         | Displays information about the PTP clock.      |
|                  | <b>show ptp parent</b>        | Displays the PTP parent properties.            |
|                  | <b>show ptp port</b>          | Displays the PTP port properties.              |
|                  | <b>show ptp time-property</b> | Displays the time properties of the PTP clock. |

# show ptp parent

To display the properties of the PTP parent, use the **show ptp parent** command in user EXEC mode.

## show ptp parent

|                           |                                            |
|---------------------------|--------------------------------------------|
| <b>Syntax Description</b> | This command has no arguments or keywords. |
|---------------------------|--------------------------------------------|

|                      |           |
|----------------------|-----------|
| <b>Command Modes</b> | User EXEC |
|----------------------|-----------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(12)MR2 | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                                                                     |
|-------------------------|-------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | Use the <b>show ptp parent</b> command to display the properties of the PTP parent. |
|-------------------------|-------------------------------------------------------------------------------------|

|                 |                                                                             |
|-----------------|-----------------------------------------------------------------------------|
| <b>Examples</b> | The following example shows output from the <b>show ptp parent</b> command: |
|-----------------|-----------------------------------------------------------------------------|

```
Router# show ptp parent
PTP PARENT PROPERTIES
  Parent Clock:
    Parent Clock Identity: 0x0:1E:4A:FF:FF:96:A9:9E
    Parent Port Number: 0
    Observed Parent Offset (log variance): N/A
    Observed Parent Clock Phase Change Rate: 0

  Grandmaster Clock:
    Grandmaster Clock Identity: 0x0:1E:4A:FF:FF:96:A9:9E
    Grandmaster Clock Quality:
      Class: 248
      Accuracy: Greater than 10s
      Offset (log variance): 52592
      Priority1: 128
      Priority2: 128
```

| Related Commands | Command                        | Description                                    |
|------------------|--------------------------------|------------------------------------------------|
|                  | show ptp clock                 | Displays information about the PTP clock.      |
|                  | show ptp foreign-master-record | Displays the PTP foreign master records.       |
|                  | show ptp port                  | Displays the PTP port properties.              |
|                  | show ptp time-property         | Displays the time properties of the PTP clock. |

# show ptp port

To display the PTP port properties, use the **show ptp port** command in user EXEC mode.

## show ptp port

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(12)MR2 | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** Use the **show ptp port** command to display the PTP port properties.

**Examples** The following example shows output from the **show ptp port** command:

```
Router# show ptp port
PTP PORT DATASET: Vlan1
  Port identity: clock identity: 0x0:1E:4A:FF:FF:96:A9:9E
  Port identity: port number: 1
  PTP version: 2
  Delay request interval(log mean): 0
  Announce receipt time out: 0
  Peer mean path delay: 0
  Announce interval(log mean): 0
  Sync interval(log mean): 0
  Delay Mechanism: End to End
  Peer delay request interval(log mean): 0
  Sync fault limit: 6000
```

| Related Commands | Command                               | Description                                    |
|------------------|---------------------------------------|------------------------------------------------|
|                  | <b>show ptp clock</b>                 | Displays information about the PTP clock.      |
|                  | <b>show ptp foreign-master-record</b> | Displays the PTP foreign master records.       |
|                  | <b>show ptp parent</b>                | Displays the PTP parent properties.            |
|                  | <b>show ptp time-property</b>         | Displays the time properties of the PTP clock. |

# show ptp time-property

To display the PTP clock time properties, use the **show ptp time-property** command in user EXEC mode.

## show ptp time-property

|                           |                                            |
|---------------------------|--------------------------------------------|
| <b>Syntax Description</b> | This command has no arguments or keywords. |
|---------------------------|--------------------------------------------|

|                      |           |
|----------------------|-----------|
| <b>Command Modes</b> | User EXEC |
|----------------------|-----------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(12)MR2 | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                                                                     |
|-------------------------|-------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | Use the <b>show ptp time-property</b> command to display PTP clock time properties. |
|-------------------------|-------------------------------------------------------------------------------------|

|                 |                                                                               |
|-----------------|-------------------------------------------------------------------------------|
| <b>Examples</b> | The following example shows output from the <b>ptp time-property</b> command: |
|-----------------|-------------------------------------------------------------------------------|

```
Router# show ptp time-property
PTP CLOCK TIME PROPERTY
  Current UTC offset valid: 1
  Current UTC offset: 33
  Leap 59: 0
  Leap 61: 0
  Time Traceable: 0
  Frequency Traceable: 1
  PTP Timescale: 1
  Time Source: Hand Set
```

| Related Commands | Command                               | Description                               |
|------------------|---------------------------------------|-------------------------------------------|
|                  | <b>show ptp clock</b>                 | Displays information about the PTP clock. |
|                  | <b>show ptp foreign-master-record</b> | Displays the PTP foreign master records.  |
|                  | <b>show ptp parent</b>                | Displays the PTP parent properties.       |
|                  | <b>show ptp port</b>                  | Displays the PTP port properties.         |

# show rep topology

Use the **show rep topology** User EXEC command to display Resilient Ethernet Protocol (REP) topology information for a segment or for all segments, including the primary and secondary edge ports in the segment.

```
show rep topology [segment segment_id] [archive] [detail] [ | {begin | exclude | include}
expression]
```

## Syntax Description

|                                     |                                                                                                                         |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>segment</b><br><i>segment-id</i> | (Optional) Display REP topology information for the specified segment. The ID range is from 1 to 1024.                  |
| <b>archive</b>                      | (Optional) Display the previous topology of the segment. This keyword can be useful for troubleshooting a link failure. |
| <b>detail</b>                       | (Optional) Display detailed REP topology information.                                                                   |
| <b>begin</b>                        | (Optional) Display begins with the line that matches the <i>expression</i> .                                            |
| <b>exclude</b>                      | (Optional) Display excludes lines that match the <i>expression</i> .                                                    |
| <b>include</b>                      | (Optional) Display includes lines that match the specified <i>expression</i> .                                          |
| <i>expression</i>                   | Expression in the output to use as a reference point.                                                                   |

## Command Modes

User EXEC

## Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(40)SE  | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

The output of this command is also included in the **show tech-support** privileged EXEC command output.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.



**Examples**

This is a sample output from the **show rep topology segment** privileged EXEC command:

```
Switch # show rep topology segment 1
REP Segment 1
BridgeName      PortName      Edge Role
-----
sw1_multseg_3750 Gi1/1/1      Pri  Alt
sw3_multseg_3400 Gi0/13       Open
sw3_multseg_3400 Gi0/14       Alt
sw4_multseg_3400 Gi0/13       Open
sw4_multseg_3400 Gi0/14       Open
sw5_multseg_3400 Gi0/13       Open
sw5_multseg_3400 Gi0/14       Open
sw2_multseg_3750 Gi1/1/2      Open
sw2_multseg_3750 Gi1/1/1      Open
sw1_multseg_3750 Gi1/1/2      Sec  Open
```

This is a sample output from the **show rep topology** command when the edge ports are configured to have no REP neighbor:

```
Switch # show rep topology
REP Segment 2
BridgeName      PortName      Edge Role
-----
sw8-ts8-51      Gi0/2         Pri*  Open
sw9-ts11-50     Gi1/0/4       Open
sw9-ts11-50     Gi1/0/2       Open
sw1-ts11-45     Gi0/2         Alt
sw1-ts11-45     Po1           Open
sw8-ts8-51      Gi0/1         Sec*  Open
```

This example shows output from the **show rep topology detail** command:

```
Router# show rep topology detail
REP Segment 2
repc_2_24ts, Fa0/2 (Primary Edge)
  Alternate Port, some vlans blocked
  Bridge MAC: 0019.e714.5380
  Port Number: 004
  Port Priority: 080
  Neighbor Number: 1 / [-10]
repc_3_12cs, Gi0/1 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a292.3580
  Port Number: 001
  Port Priority: 000
  Neighbor Number: 2 / [-9]
repc_3_12cs, Po10 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a292.3580
  Port Number: 080
  Port Priority: 000
  Neighbor Number: 3 / [-8]
repc_4_12cs, Po10 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a19d.7c80
  Port Number: 080
  Port Priority: 000
  Neighbor Number: 4 / [-7]
repc_4_12cs, Gi0/2 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 001a.a19d.7c80
  Port Number: 002
  Port Priority: 040
```

## show rep topology

Neighbor Number: 5 / [-6]

<output truncated>

This example shows output from the **show rep topology segment archive** command:

```
Router# show rep topology segment 1 archive
REP Segment 1
BridgeName      PortName      Edge Role
-----
sw1_multseg_3750 Gi1/1/1      Pri  Open
sw3_multseg_3400 Gi0/13              Open
sw3_multseg_3400 Gi0/14              Open
sw4_multseg_3400 Gi0/13              Open
sw4_multseg_3400 Gi0/14              Open
sw5_multseg_3400 Gi0/13              Open
sw5_multseg_3400 Gi0/14              Open
sw2_multseg_3750 Gi1/1/2              Alt
sw2_multseg_3750 Gi1/1/1              Open
sw1_multseg_3750 Gi1/1/2      Sec  Open
```

### Related Commands

| Command            | Description                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>rep segment</b> | Enables REP on an interface and assigns a segment ID. This command is also used to configure a port as an edge port, a primary edge port, or a preferred port. |

# show xconnect

To display information about xconnect attachment circuits and pseudowires (PWs), use the **show xconnect all** command in privileged EXEC mode.

**show xconnect** { **all** | **interface** *interface* | **peer** *ip-address* { **all** | **vcid** *vcid* } } [**detail**]

| Syntax Description                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>all</b>                                                             | Displays information about all xconnect attachment circuits and PWs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>interface</b> <i>interface</i>                                      | Displays information about xconnect attachment circuits and PWs on the specified interface. Valid values for the argument are as follows: <ul style="list-style-type: none"> <li><b>atm number</b>—Displays xconnect information for a specific ATM interface or subinterface.</li> <li><b>atm number vp vpi-value</b>—Displays virtual path (VP) xconnect information for a specific ATM virtual path identifier (VPI). This command does not display information about virtual connect (VC) xconnects using the specified VPI.</li> <li><b>atm number vp vpi-value/vci-value</b>—Displays VC xconnect information for a specific ATM VPI and virtual circuit identifier (VCI) combination.</li> <li><b>serial number</b>—Displays xconnect information for a specific serial interface.</li> <li><b>serial number dlci-number</b>—Displays xconnect information for a specific Frame Relay data-link connection identifier (DLCI).</li> <li><b>vlan vlan-number</b>—Displays vlan-mode xconnect information for a specific VLAN interface.</li> </ul> |
| <b>peer</b> <i>ip-address</i> { <b>all</b>   <b>vcid</b> <i>vcid</i> } | Displays information about xconnect attachment circuits and PWs associated with the specified peer IP address. <ul style="list-style-type: none"> <li><b>all</b>—Displays all xconnect information associated with the specified peer IP address.</li> <li><b>vcid vcid</b>—Displays xconnect information associated with the specified peer IP address and the specified VC ID.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>detail</b>                                                          | (Optional) Displays detailed information about the specified xconnect attachment circuits and PWs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

**Command Modes** Privileged EXEC

| Command History | Release     | Modification                                                                                                 |
|-----------------|-------------|--------------------------------------------------------------------------------------------------------------|
|                 | 12.0(31)S   | This command was introduced.                                                                                 |
|                 | 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.                                               |
|                 | 12.4(11)T   | This command was integrated into Cisco IOS Release 12.4(11)T.                                                |
|                 | 12.2(33)SRB | This command was updated with the <b>rib</b> keyword.                                                        |
|                 | 12.2(33)SRC | This command was updated to add SB=Standby and RV=Recovering to the State of the Segment in output displays. |
|                 | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI.                                              |

| Release                  | Modification                                                    |
|--------------------------|-----------------------------------------------------------------|
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1.      |
| 12.4(19)MR2              | This command was integrated into Cisco IOS Release 12.4(19)MR2. |
| 12.2(33)MRA              | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

### Usage Guidelines

The **show xconnect all** command can be used to display, sort, and filter basic information about all xconnect attachment circuits and PWs.

You can use the **show xconnect all** command output to help determine the appropriate steps to troubleshoot an xconnect configuration problem. More specific information about a particular type of xconnect can be displayed using the commands listed in the Related Commands table.

### Examples

The following example shows **show xconnect all** command output in the brief (default) display format. The output shows information about the interfaces and VCs that have been configured to transport various Layer 2 packets on the router.

```
Router# show xconnect all
```

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State

UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware

XC ST Segment 1 S1 Segment 2 S2

```

-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
ST      Segment 1                               S1 Segment 2                               S2
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
UP      ac      Et0/0(Ethernet)                   UP mpls 10.55.55.2:1000                               UP
UP      ac      Et1/0.1:200(Eth VLAN)              UP mpls 10.55.55.2:5200                               UP
IA pri  ac      Et1/0.2:100(Eth VLAN)              UP ac      Et2/0.2:100(Eth VLAN)                       UP
UP sec  ac      Et1/0.2:100(Eth VLAN)              UP mpls 10.55.55.3:1101                               UP

```

Table B-52 describes the significant fields shown in the display.

**Table B-52** *show xconnect all Field Descriptions*

| Field | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| XC ST | <p>State of the xconnect attachment circuit or PW. Valid states are:</p> <ul style="list-style-type: none"> <li>UP—The xconnect attachment circuit or PW is up. Both segment 1 and segment 2 must be up for the xconnect to be up.</li> <li>DN—The xconnect attachment circuit or PW is down. Either segment 1, segment 2, or both segments are down.</li> <li>IA—The xconnect attachment circuit or PW is inactive. This state is valid only when PW redundancy is configured.</li> <li>NH—One or both segments of this xconnect no longer has the required hardware resources available to the system.</li> </ul> |

**Table B-52** *show xconnect all Field Descriptions (continued)*

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Segment 1<br>or<br>Segment 2 | Information about the type of xconnect, the interface type, and the IP address the segment is using. Types of xconnects are: <ul style="list-style-type: none"> <li>ac—Attachment circuit.</li> <li>pri ac—Primary attachment circuit.</li> <li>sec ac—Secondary attachment circuit.</li> <li>mpls—Multiprotocol Label Switching.</li> <li>l2tp—Layer 2 Tunnel Protocol.</li> </ul> |
| S1<br>or<br>S2               | State of the segment. Valid states are: <ul style="list-style-type: none"> <li>UP—The segment is up.</li> <li>DN—The segment is down.</li> <li>AD—The segment is administratively down.</li> </ul>                                                                                                                                                                                  |

The following example shows **show xconnect all** command output in the detailed display format:

Router# **show xconnect all detail**

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State

UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No HardwareXC

| ST | Segment 1                                          | S1 | Segment 2                                                                            | S2 |
|----|----------------------------------------------------|----|--------------------------------------------------------------------------------------|----|
| UP | ac Et0/0(Ethernet)<br>Interworking: ip             | UP | mpls 10.55.55.2:1000<br>Local VC label 16<br>Remote VC label 16<br>pw-class: mpls-ip | UP |
| UP | ac Et1/0.1:200(Eth VLAN)<br>Interworking: ip       | UP | mpls 10.55.55.2:5200<br>Local VC label 17<br>Remote VC label 20<br>pw-class: mpls-ip | UP |
| IA | pri ac Et1/0.2:100(Eth VLAN)<br>Interworking: none | UP | ac Et2/0.2:100(Eth VLAN)<br>Interworking: none                                       | UP |
| UP | sec ac Et1/0.2:100(Eth VLAN)<br>Interworking: none | UP | mpls 10.55.55.3:1101<br>Local VC label 23<br>Remote VC label 17<br>pw-class: mpls    | UP |

The additional fields displayed in the detailed output are self-explanatory.

**Related Commands**

| Command                     | Description                                                                                                 |
|-----------------------------|-------------------------------------------------------------------------------------------------------------|
| <b>show atm pvc</b>         | Displays all ATM PVCs and traffic information.                                                              |
| <b>show atm vc</b>          | Displays all ATM PVCs and SVCs and traffic information.                                                     |
| <b>show atm vp</b>          | Displays the statistics for all VPs on an interface or for a specific VP.                                   |
| <b>show connect</b>         | Displays configuration information about drop-and-insert connections that have been configured on a router. |
| <b>show frame-relay pvc</b> | Displays statistics about PVCs for Frame Relay interfaces.                                                  |
| <b>show interfaces</b>      | Displays statistics for all interfaces configured on the router or access server.                           |

| Command                              | Description                                                                                      |
|--------------------------------------|--------------------------------------------------------------------------------------------------|
| <b>show mpls l2transport binding</b> | Displays VC label binding information.                                                           |
| <b>show mpls l2transport vc</b>      | Displays information about AToM VCs that have been enabled to route Layer 2 packets on a router. |

# signaling

Specifies the signaling type used on a CEM interface. To disable a signaling configuration, use the **no** form of this command.

**signaling [inband-cas]**

**no signaling [inband-cas]**

|                           |                                                                                             |
|---------------------------|---------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>inband-cas</b> Specifies inband channel-associated signaling (CAS) on the CEM interface. |
|---------------------------|---------------------------------------------------------------------------------------------|

|                        |                                      |
|------------------------|--------------------------------------|
| <b>Command Default</b> | This command is disabled by default. |
|------------------------|--------------------------------------|

|                      |                             |
|----------------------|-----------------------------|
| <b>Command Modes</b> | CEM interface configuration |
|----------------------|-----------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                             |
|------------------------|----------------|-----------------------------------------------------------------|
|                        | 12.4(20)MR     | This command was introduced.                                    |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA. |
|                        |                |                                                                 |

|                 |                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------|
| <b>Examples</b> | The following example shows how the signaling command is used in an E1 controller configuration. |
|-----------------|--------------------------------------------------------------------------------------------------|

```
Router(config-if)# controller e1 0/0
Router(config-controller)# mode cas
Router(config-controller)# cem-group 0 timeslots 1-31
Router(config-controller)# interface CEM 0/0
Router(config-if)# cem 0
Router(config-if-cem)# signaling inband-cas
Router(config-if-cem)# xconnect 30.30.30.2 305 encapsulation mpls
```

| <b>Related Commands</b> | <b>Command</b>    | <b>Description</b>                                                                                                 |
|-------------------------|-------------------|--------------------------------------------------------------------------------------------------------------------|
|                         | <b>cem-group</b>  | Creates a circuit emulation (CEM) channel from one or more time slots of a T1 or E1 line.                          |
|                         | <b>controller</b> | Configures a T1, E1, or BITS controller and enters controller configuration mode.                                  |
|                         | <b>mode cas</b>   | Allows you to specify the controller mode for ATM, T1, or E1 controllers and enters controller configuration mode. |

# snmp-server enable traps ethernet cfm alarm

To enable Ethernet Connectivity Fault Management (CFM) fault alarm traps, use the **snmp-server enable traps ethernet cfm alarm** command in global configuration mode. To disable fault alarm traps, use the **no** form of this command.

- snmp-server enable traps ethernet cfm alarm**
- no snmp-server enable traps ethernet cfm alarm**

Syntax Description

This command has no arguments or keywords.

Command Default

Traps are disabled.

Command Modes

Global configuration (config)

Command History

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.2(33)SRD | This command was introduced.                                    |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

Usage Guidelines

Use this command to turn on or turn off CFM fault alarm traps.

Examples

The following example shows how to enable CFM fault alarm traps:

```
Router#
Router(config)# snmp-server enable traps ethernet cfm alarm
```



## snmp-server enable traps ethernet cfm cc

To enable Simple Network Management Protocol (SNMP) trap generation for Ethernet connectivity fault management (CFM) continuity check events, use the **snmp-server enable traps ethernet cfm cc** command in global configuration mode. To disable SNMP trap generation for Ethernet CFM continuity check events, use the **no** form of this command.

**snmp-server enable traps ethernet cfm cc** [**config**] [**cross-connect**] [**loop**] [**mep-down**] [**mep-up**]

**no snmp-server enable traps ethernet cfm cc** [**config**] [**cross-connect**] [**loop**] [**mep-down**] [**mep-up**]

| Syntax Description   |                                                                                                                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>config</b>        | (Optional) Generates a trap when a CFM misconfiguration exists in the network.                                                                                                                          |
| <b>cross-connect</b> | (Optional) Generates a trap when a cross-connected service exists in the network.                                                                                                                       |
| <b>loop</b>          | (Optional) Generates a trap when a forwarding loop exists in the network.                                                                                                                               |
| <b>mep-down</b>      | (Optional) Generates a trap when a device has lost connectivity with a remote MEP or when connectivity from a previously learned remote MEP is restored after interruption.                             |
| <b>mep-up</b>        | (Optional) Generates a trap when a new remote maintenance endpoint (MEP) has been discovered and learned by the device or when a change occurs in the port state of a previously discovered remote MEP. |

**Command Default** When no options are configured, all continuity check traps are enabled.

**Command Modes** Global configuration (config)

| Command History | Release      | Modification                                                     |
|-----------------|--------------|------------------------------------------------------------------|
|                 | 12.2(33)SRA  | This command was introduced.                                     |
|                 | 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T.    |
|                 | 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.  |
|                 | 12.2(33)SXI2 | This command was integrated into Cisco IOS Release 12.2(33)SXI2. |
|                 | 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.  |

**Usage Guidelines** The configuration error trap (cEtherCfmCcConfigError) is triggered when a device receives a CCM that has the same MPID as a locally configured MEP but a different source MAC Address than its own. The configuration error trap includes the following fields:

- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.
- The MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.

- MPID of local MEP that has the same ID as that received in the CCM.
- Name of the interface on which the MEP above is configured.
- MAC Address of the remote device sending the CCM.

The cross-connect service trap (cEtherCfmCcCrossconnect) is generated when a device receives a continuity check message (CCM) whose service ID is different from what is locally configured on the device for the given service VLAN (S-VLAN). This mismatch indicates that there could be a cross-connected service in the network. The trap includes the following fields:

- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.
- The MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.
- MPID of remote MEP causing the alarm to be raised.
- MAC address of remote MEP causing the alarm to be raised.
- Service ID reported by the remote MEP.

The loop trap (cEtherCfmCcLoop) is generated when a device receives a CCM that has the same source MAC Address and MPID as its own, thereby indicating that the device is receiving its own CCMs and that a forwarding loop exists in the network. The loop trap includes the following fields:

- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.
- The MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.
- MPID of the MEP originating the CCM.
- Name of the interface on which the MEP above is configured.

The mep-down trap (cEtherCfmCcMepDown) notifies the NMS that the device has lost connectivity with a remote MEP. This trap also serves as a clear for Loop, Config, Cross-Connect and Unknown-MEP events.

The mep-down trap is generated in the following cases:

- A valid CCM with a zero hold-time is received from a remote MEP, and the device either has a valid (non-expired) CCDB entry for that MEP or does not have any CCDB entry. In other words, the trap is not generated for an already expired CCDB entry. This trigger has the event code “lastGasp.”
- An entry for a remote MEP in the CCDB expires and is archived. This trigger has the event code “timeout.”
- A previous configuration error trap is cleared. This trigger has the event code “configClear.”
- A previous loop trap is cleared. This trigger has the event code “loopClear.”
- A previous Crossconnect trap is cleared. This trigger has the event code “xconnectClear.”
- A previous unknown trap is cleared. This trigger has the event code “unknownClear.”

The mep-down trap includes the following fields:

- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.
- The MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.
- A count of the local MEPs on the same domain and S-VLAN as the remote MEP that are affected by the event.
- A count of the different interfaces on which the local MEPs above are configured.

- MPID of the remote MEP that is being reported down.
- MAC address of the remote MEP that is being reported down.
- Event code indicating one of the following: lastGasp, timeout, configClear, loopClear, xconnectClear, unknownClear.

The mep-up trap (cEtherCfmCcMepUp) serves three functions. One function is to notify the network management system (NMS) that a new MEP has been discovered and learned by the device. The second function is that the trap notifies the NMS that there is a change in the port-state of a previously discovered remote MEP. The third is to notify the NMS when connectivity from a previously discovered MEP is restored after interruption.

Mep-up traps are suppressed while cross-check is operational because the cross-check traps more efficiently convey the status of the service.

The mep-up trap is generated in the following cases:

- A valid CCM with a non-zero hold-time is received from a remote MEP for the first time, and hence an entry is created for that MEP in the continuity check database (CCDB). This trigger has the event code "new."
- A valid CCM with a non-zero hold-time is received from a remote MEP for which the device has an expired entry in the CCDB (that is, the device has an entry for that remote MEP in the archived DB). This trigger has the event code "returning."
- A valid CCM with a non-zero hold-time is received from a remote MEP for which the device has a valid entry in the CCDB and the port-state indicated in the CCM is different from what is cached in the CCDB. This trigger has the event code "portState"

The mep-up trap includes the following fields:

- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.
- The MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.
- A count of the local MEPs on the same domain and S-VLAN as the remote MEP that are affected by the event.
- A count of the different interfaces on which the local MEPs above are configured.
- MPID of the remote MEP that is being reported up.
- MAC address of the remote MEP that is being reported up.
- Event code indicating one of the following: new MEP, returning MEP, or port-state change.
- Port state of remote MEP.

## Examples

The following example shows how to enable SNMP trap generation for Ethernet CFM continuity checks when a new remote MEP is discovered and learned by the device:

```
Router(config)# snmp-server enable traps ethernet cfm cc mep-up
```

# snmp-server enable traps ethernet cfm crosscheck

To enable Simple Network Management Protocol (SNMP) trap generation for Ethernet connectivity fault management (CFM) continuity check events, in relation to the cross-check operation between statically configured maintenance endpoints (MEPs) and those learned via continuity check messages (CCMs), use the **snmp-server enable traps ethernet cfm crosscheck** command in global configuration mode. To disable SNMP trap generation for these continuity check events, use the **no** form of this command.

**snmp-server enable traps ethernet cfm crosscheck [mep-missing] [mep-unknown] [service-up]**

**no snmp-server enable traps ethernet cfm crosscheck [mep-missing] [mep-unknown] [service-up]**

## Syntax Description

|                    |                                                                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mep-missing</b> | (Optional) Generates a trap when the cross-check enable timer expires and no CCMs were received from an expected (configured) MEP. One trap is generated per remote MEP. |
| <b>mep-unknown</b> | (Optional) Generates a trap when an unexpected (unconfigured) MEP comes up. One trap is generated per remote MEP.                                                        |
| <b>service-up</b>  | (Optional) Generates a trap when all remote MEPs belonging to a service instance come up.                                                                                |

## Command Default

This command is disabled.

When no options are configured, all continuity check event traps are enabled.

## Command Modes

Global configuration (config)

## Command History

| Release      | Modification                                                     |
|--------------|------------------------------------------------------------------|
| 12.2(33)SRA  | This command was introduced.                                     |
| 12.4(11)T    | This command was integrated into Cisco IOS Release 12.4(11)T.    |
| 12.2(33)SXH  | This command was integrated into Cisco IOS Release 12.2(33)SXH.  |
| 12.2(33)SX12 | This command was integrated into Cisco IOS Release 12.2(33)SX12. |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA.  |

## Usage Guidelines

For this class of traps to function, cross-check must be enabled on the device. Otherwise, none of these traps are generated, even if they are configured.

The mep-missing trap (cEtherCfmXCheckMissing) notifies the network management system (NMS) that the device did not receive any CCMs from a remote MEP that it was expecting to be part of the service instance.

The mep-missing trap is generated in the following case:

- After enabling cross-check (**ethernet cfm mep crosscheck enable**), the device waits for the cross-check-start timeout value specified (**ethernet cfm mep crosscheck enable-timeout**). When the timeout period has elapsed, the device cross-checks the list of remote MEPs it has learned via CCMs against the static list that has been configured (**mep crosscheck mpid vlan**). For each remote MEP that is configured in the static list and for which the device has not received a CCM, a mep-missing trap is generated. The mep-missing trap has the following fields:
- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.
- MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.
- MPID of the remote MEP that is being reported missing.
- MAC address of the remote MEP that is being reported missing.

The mep-unknown trap (cEtherCfmXCheckUnknown) notifies the NMS that the device received CCMs from a remote MEP that it was not expecting to be part of the service instance.

The mep-unknown trap is generated in the following case:

- After cross-check is in an operational state, the device dynamically examines the list of statically configured remote MEPs against what it learns from CCMs. This occurs after cross-check is enabled and the timer has expired. When the device receives a CCM with non-zero hold time from a remote MEP that does not exist in the static list, the device raises a mep-unknown trap.

The mep-unknown trap has the following fields:

- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.
- MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.
- MPID of the remote MEP that is being reported unknown.
- MAC address of the remote MEP that is being reported unknown.

The service-up trap (cEtherCfmXCheckServiceUp) notifies the NMS that the device received CCMs from all remote MEPs within a given service instance.

The service-up trap is generated in the following case:

- When the device receives CCMs from all remote statically configured MEPs before the expiration of the crosscheck enable-timeout period.

The service-up trap has the following fields:

- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.
- MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.

## Examples

The following example shows how to enable SNMP trap generation for Ethernet CFM continuity check events when an unexpected (unconfigured) MEP comes up:

```
Router (config)# snmp-server enable traps ethernet cfm crosscheck mep-unknown
```

| Related Commands | Command                                   | Description                                                                                                  |
|------------------|-------------------------------------------|--------------------------------------------------------------------------------------------------------------|
|                  | <b>ethernet cfm mep crosscheck enable</b> | Enables cross checking between the list of configured remote MEPs of a domain and MEPs learned through CCMs. |
|                  | <b>mep crosscheck mpid vlan</b>           | Statically defines a remote MEP within a maintenance domain.                                                 |

# switch l2trust

Enables layer 2 trust mode on the Cisco MWR 2941 gigabitEthernet ports. To disable layer 2 trust mode, use the **no** form of this command.

**switch l2trust**

**no switch l2trust**

|                        |                                      |
|------------------------|--------------------------------------|
| <b>Command Default</b> | This command is disabled by default. |
|------------------------|--------------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(20)MR  | This command was introduced.                                    |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

|                         |                                                                                                |
|-------------------------|------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | This command enables layer 2 trusted mode for all gigabitEthernet ports on the Cisco MWR 2941. |
|-------------------------|------------------------------------------------------------------------------------------------|

|                 |                                                                   |
|-----------------|-------------------------------------------------------------------|
| <b>Examples</b> | The following example shows the output generated by this command: |
|-----------------|-------------------------------------------------------------------|

```
Router(config)# switch l2trust
Router(config)# exit
```

| Related Commands | Command                                 | Description                                              |
|------------------|-----------------------------------------|----------------------------------------------------------|
|                  | <b>show interface switchport backup</b> | Displays status information about the backup switchport. |

# switchport backup

Use the **switchport backup interface** interface configuration command on a Layer 2 interface to configure Flex Links, a pair of interfaces that provide backup to each other. Use the **no** form of this command to remove the Flex Links configuration.

```
switchport backup interface {interface-id}

no switchport backup interface {interface-id}
```

|                    |              |                                                                                                                                                                                    |
|--------------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | interface-id | The Layer 2 interface that acts as a backup link to the interface being configured. The interface can be a physical interface or port channel. The port-channel range is 1 to 486. |
|--------------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                              |
|-----------------|------------------------------|
| Command Default | There is no default setting. |
|-----------------|------------------------------|

|               |                         |
|---------------|-------------------------|
| Command Modes | Interface configuration |
|---------------|-------------------------|

|                 |             |                                                                       |
|-----------------|-------------|-----------------------------------------------------------------------|
| Command History | Release     | Modification                                                          |
|                 | 12.2(18)SXF | Support for this command was introduced on the Supervisor Engine 720. |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.       |
|                 | 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2.       |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.       |

Examples

The following example shows the output generated by this command:

Router(config)# interface gigabitethernet0/3  
Router(config-if)# switchport backup interface gigabitethernet0/4  
Router(config-if)# exit  
Router(config)# exit



| Related Commands | Command                                 | Description                                              |
|------------------|-----------------------------------------|----------------------------------------------------------|
|                  | <b>show interface switchport backup</b> | Displays status information about the backup switchport. |

# switchport stacking-partner

Stacking allows you to configure two switch modules in a single chassis to behave as a single switch. This is done by selecting one port from each switch module and configuring it to be a stacking partner. You must then use a cable to connect the stacking partners from each switch module to physically stack the switch modules. Any one port in a switch module can be designated as the stacking partner for that switch module.

Use the **switchport stacking-partner** command to configure a stacking partner port. You can use this command on the onboard gigabitEthernet ports or on fastEthernet ports on the HWIC-D-9ESW card. Use the **no** form of this command to remove the configuration.

**switchport stacking-partner interface gigabitethernet *partner-interface-id***

**no switchport stacking-partner interface gigabitethernet *partner-interface-id***

|                           |                             |                                                                          |
|---------------------------|-----------------------------|--------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>interface</b>            | Specifies the stacking partner interface.                                |
|                           | <b>gigabitethernet</b>      |                                                                          |
|                           | <i>partner-interface-id</i> | The slot and port number of the stacking partner interface, such as 0/1. |

|                        |       |
|------------------------|-------|
| <b>Command Default</b> | None. |
|------------------------|-------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | Interface configuration |
|----------------------|-------------------------|

|                        |                |                                                                 |
|------------------------|----------------|-----------------------------------------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                             |
|                        | 12.3(8)T4      | This command was introduced.                                    |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.  |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Examples** The following example shows the output generated by this command:

```
Router(config)# interface gigabitethernet0/3
Router(config-if)# switchport stacking-partner interface gigabitethernet0/4
```

|                         |                                  |                                                   |
|-------------------------|----------------------------------|---------------------------------------------------|
| <b>Related Commands</b> | <b>Command</b>                   | <b>Description</b>                                |
|                         | <b>show interface switchport</b> | Displays status information about the switchport. |

# traceroute ethernet

To send Ethernet connectivity fault management (CFM) traceroute messages to a destination maintenance endpoint (MEP), use the **traceroute ethernet** command in privileged EXEC mode. This command does not have a **no** form.

**traceroute ethernet** *mac-address* { **domain** *domain-name* { **vlan** *vlan-id* | **level** *level-id* }

traceroute ethernet mac-address { domain domain-name vlan vlan-id | level level-num vlan vlan-id }

## Syntax Description

|                    |                                                                   |
|--------------------|-------------------------------------------------------------------|
| <i>mac-address</i> | MAC address of a remote MEP in the format abcd.abcd.abcd.         |
| <b>domain</b>      | Specifies the domain in which the destination MEP resides.        |
| <i>domain-name</i> | String of a maximum of 154 characters that identifies the domain. |
| <b>vlan</b>        | Specifies a VLAN.                                                 |
| <i>vlan-id</i>     | Integer from 1 to 4094 that identifies the VLAN.                  |
| <b>level</b>       | Indicates a maintenance level is specified.                       |
| <i>level-id</i>    | Integer from 0 to 7 that identifies the maintenance level.        |

## Command Modes

Privileged EXEC (#)

## Command History

| Release      | Modification                                                    |
|--------------|-----------------------------------------------------------------|
| 12.2(33)SX12 | This command was introduced.                                    |
| 12.2(33)MRA  | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

## Usage Guidelines

If a CoS is not configured, the default is the highest priority allowed for the egress interface.

FDB is another term for the L2 forwarding table. When the **fdb-only** option is configured, only MAC addresses learned in a bridge's FDB (not information saved in the maintenance intermediate point [MIP] continuity check database [CCDB]) are used to determine the egress port.

The destination can be either a MEP or a MIP. If the destination is a MIP, the FDB must have a MAC address entry for that MIP; that is, the FDB has learned the MIP's MAC address via Linktrace responses.

For a bridge domain-VLAN service, the VLAN ID can be used to initiate traceroute.

The following example shows a **traceroute ethernet** command and output:

```
Router# traceroute ethernet 1.1.1 domain Domain_L5 vlan 9
```

```
Type escape sequence to abort. TTL 64. Linktrace Timeout is 5 seconds
Tracing the route to aabb.cc03.bb99 on Domain Domain_L5, Level 5, vlan 9
Traceroute sent via Ethernet0/0.9, path found via MPDB
```

```
B = Intermediary Bridge
! = Target Destination
* = Per hop Timeout
```

```
-----
Hops      Host                MAC      Ingress    Ingr Action  Relay Action
              Forwarded    Egress    Egr Action  Previous Hop
```

```
-----
! 1          aabb.cc03.bb99          RlyHit:MEP
          Not Forwarded          aabb.cc03.b999
```

|                  |                                     |                                                                           |
|------------------|-------------------------------------|---------------------------------------------------------------------------|
| Related Commands | Command                             | Description                                                               |
|                  | clear ethernet cfm errors           | Removes continuity check error conditions from the error database.        |
|                  | clear ethernet cfm traceroute-cache | Removes the contents of the traceroute cache.                             |
|                  | ethernet cfm traceroute-cache       | Enables caching of Ethernet CFM data learned through traceroute messages. |
|                  | show ethernet traceroute-cache      | Displays the contents of the traceroute cache.                            |

# tunnel destination

To specify the destination for a tunnel interface, use the **tunnel destination** command in interface configuration mode. To remove the destination, use the **no** form of this command.

**tunnel destination** {*host-name* | *ip-address*}

**no tunnel destination**

|                           |                   |                                                                          |
|---------------------------|-------------------|--------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>host-name</i>  | Name of the host destination.                                            |
|                           | <i>ip-address</i> | IP address of the host destination expressed in dotted decimal notation. |

|                        |                                               |
|------------------------|-----------------------------------------------|
| <b>Command Default</b> | No tunnel interface destination is specified. |
|------------------------|-----------------------------------------------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | Interface configuration |
|----------------------|-------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                                                               |
|------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | 10.0           | This command was introduced.                                                                                                                                                      |
|                        | 12.3(7)T       | The address field was modified to accept an <i>ipv6-address</i> argument to allow IPv6 nodes to be configured as a tunnel destination.                                            |
|                        | 12.2(30)S      | This command was integrated into Cisco IOS Release 12.2(30)S.                                                                                                                     |
|                        | 12.2(28)SB     | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                                                                    |
|                        | 12.2(25)SG     | This command was integrated into Cisco IOS Release 12.2(25)SG.                                                                                                                    |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                        | 12.2SX         | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

|                         |                                                                                                                                                                                                                                           |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | You cannot configure two tunnels to use the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and configure the packet source off of the loopback interface. |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | <b>Tunnel Destination Address for GRE Tunneling Example</b>                                                                        |
|                 | The following generic routing encapsulation (GRE) example shows how to configure the tunnel destination address for GRE tunneling: |

```
Router(config)# interface tunnel0
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode gre ip
```

■ tunnel destination

| Related Commands | Command       | Description                                           |
|------------------|---------------|-------------------------------------------------------|
|                  | tunnel mode   | Sets the encapsulation mode for the tunnel interface. |
|                  | tunnel source | Sets the source address of a tunnel interface.        |

# tunnel source

To set the source address for a tunnel interface, use the **tunnel source** command in interface configuration mode. To remove the source address, use the **no** form of this command.

**tunnel source** {*ip-address* | *interface-type interface-number*}

**no tunnel source**

|                           |                         |                                                                                                                                                                                                        |
|---------------------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>ip-address</i>       | IP address to use as the source address for packets in the tunnel.                                                                                                                                     |
|                           | <i>interface-type</i>   | Interface type.                                                                                                                                                                                        |
|                           | <i>interface-number</i> | Port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system and can be displayed with the <b>show interfaces</b> command. |

**Command Default** No tunnel interface source address is set.

**Command Modes** Interface configuration

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                                                                                                                               |
|------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | 10.0           | This command was introduced.                                                                                                                                                      |
|                        | 12.3(7)T       | The address field has been updated to accept IPv6 addresses as the source address to allow an IPv6 node to be used as a tunnel source.                                            |
|                        | 12.2(30)S      | This command was integrated into Cisco IOS Release 12.2(30)S.                                                                                                                     |
|                        | 12.2(25)SG     | This command was integrated into Cisco IOS Release 12.2(25)SG.                                                                                                                    |
|                        | 12.2(33)SRA    | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                        | 12.2SX         | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                        | 12.4(20)MR     | This command was integrated into Cisco IOS Release 12.4(20)MR.                                                                                                                    |
|                        | 12.2(33)MRA    | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                   |

**Usage Guidelines** The source address is either an explicitly defined IP address or the IP address assigned to the specified interface.

You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

Examples

GRE Tunneling Example

The following example shows how to set a tunnel source address for generic routing encapsulation (GRE) tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 172.32.164.19
Router(config-if)# tunnel mode gre ip
```

Related Commands

| Command            | Description                                       |
|--------------------|---------------------------------------------------|
| tunnel destination | Specifies the destination for a tunnel interface. |



# tx-limit

To specify the number of transmit buffers for an ATM virtual circuit (VC), use the **tx-limit** command in ATM VC, VC-bundle, VC-class, or VC-range configuration mode. To reset the number of transmit buffers for a particular VC to the default value, use the **no** form of this command.

**tx-limit** *buffers*

**no tx-limit**

## Syntax Description

|                |                                                                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>buffers</i> | Specifies the number of buffers to be used for this VC. The valid range is 2 to 57343, with a default value that is based on the current VC line rate. |
| <b>Note</b>    | Avoid configuring the <i>buffer</i> value as 1, as this can cause a traffic error on the Cisco MWR 2941.                                               |

## Command Default

Automatically computed from the VC line rate to produce a default latency of 100 milliseconds (or whatever value is specified by the **atm tx-latency** command).

## Command Modes

Interface-ATM-VC configuration (for an ATM VC)  
VC-bundle configuration  
VC-class configuration  
VC-range configuration

## Command History

| Release     | Modification                                                                                                                       |
|-------------|------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(18)SXE | This command was introduced for the ATM Shared Port Adapters (SPA) on Catalyst 6500 series switches and Cisco 7600 series routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                    |
| 12.2(33)MRB | This command was integrated into Cisco IOS Release 12.2.(33)MRB.                                                                   |

## Usage Guidelines

When you configure a VC on an ATM SPA interface, the Cisco IOS software automatically determines the maximum number of transmit buffers that are needed by the VC for its outgoing traffic. The Cisco IOS software uses both the configured VC line rate and latency value to calculate the number of buffers. Each transmit buffer can contain an ATM cell (53 bytes).

By default, each VC uses the latency value that is specified by the **atm tx-latency** command, which defaults to 100 milliseconds. The maximum number of transmit buffers is then calculated, so that traffic at the maximum VC line rate can still be transmitted within this latency value.

If a particular VC's traffic flow requires a different latency value, use the **tx-limit** command to manually configure the number of transmit buffers for that VC. This allows you to fine-tune the latency value on a per-VC basis, without affecting the other VCs on the interface.

**Tip**

Use the **atm tx-latency** command to specify the default latency value for all VCs on the interface, and then use the **tx-limit** command to fine-tune the configuration for a particular VC, as needed.

**Note**

The number of buffers can also be affected by the packet size, because each VC is always allowed to transmit at least one packet, regardless of the number of buffers configured with the **tx-limit** command. If the number of buffers specified by the **tx-limit** command is very small, and the VC must transmit a very large packet, the interface can increase the number of buffers for the VC to whatever number can accommodate the packet's size. This means that occasionally, the number of buffers can grow to whatever number can accommodate a packet up to the maximum MTU size.

**Note**

Other ATM interfaces have used the **tx-ring-limit** command to achieve a similar result, but this command is not supported on ATM SPA interfaces, because it does not apply to the SPA architecture.

**Examples**

The following example shows an ATM VC being configured for a maximum of 500 buffers:

```
Router# configure terminal
Router(config)# interface atm 4/0/0.10 point-to-point
Router(config-subif)# pvc 10/101
Router(config-if-atm-vc)# tx-limit 500
Router(config-if-atm-vc)#
```

The following example shows an ATM VC being reset for its default buffer value, which is whatever buffer size is needed, at the VC line rate, to produce a default latency of 100 milliseconds (or whatever value is specified by the **atm tx-latency** command):

```
Router# configure terminal
Router(config)# interface atm 3/0/1.10 point-to-point
Router(config-subif)# pvc 10/20
Router(config-if-atm-vc)# no tx-limit
Router(config-if-atm-vc)#
```

**Related Commands**

| Command               | Description                                                                            |
|-----------------------|----------------------------------------------------------------------------------------|
| <b>atm tx-latency</b> | Specifies the default transmit latency for an ATM Shared Port Adapter (SPA) interface. |

# xconnect

To bind an attachment circuit to a pseudowire, use the **xconnect** command in one of the supported configuration modes. To restore the default values, use the **no** form of this command.

```
xconnect peer-ip-address vc-id {encapsulation {mpls [manual]} | pw-class pw-class-name}
[pw-class pw-class-name] [sequencing {transmit | receive | both}] [one-to-one |
ignore-vpi-vci]
```

```
no xconnect
```

| Syntax Description                      |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>peer-ip-address</i>                  | IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable.                                                                                                                                                                                                                                                                                                       |
| <i>vcid</i>                             | The 32-bit identifier of the virtual circuit (VC) between the PE routers.                                                                                                                                                                                                                                                                                                                                                       |
| <b>encapsulation</b>                    | <ul style="list-style-type: none"> <li><b>mpls</b>—Specifies Multiprotocol Label Switching (MPLS) as the tunneling method.</li> <li><b>manual</b>—Specifies that no signaling is to be used in the attachment circuit. This keyword places the router in xconnect configuration mode for manual configuration of the attachment circuit. Use this keyword to manually configure an AToM or L2TPv3 static pseudowire.</li> </ul> |
| <b>pw-class</b><br><i>pw-class-name</i> | (Optional) Specifies the pseudowire class for advanced configuration.                                                                                                                                                                                                                                                                                                                                                           |
| <b>sequencing</b>                       | (Optional) Sets the sequencing method to be used for packets received or sent. This keyword is not supported with the AToM Static Pseudowire Provisioning feature.                                                                                                                                                                                                                                                              |
| <b>transmit</b>                         | Sequences data packets received from the attachment circuit.                                                                                                                                                                                                                                                                                                                                                                    |
| <b>receive</b>                          | Sequences data packets sent into the attachment circuit.                                                                                                                                                                                                                                                                                                                                                                        |
| <b>both</b>                             | Sequences data packets that are both sent and received from the attachment circuit.                                                                                                                                                                                                                                                                                                                                             |
| <b>one-to-one</b>                       | Applies only when the xconnect command is configured under the AAL0 encapsulation PVC. The keyword specifies the PW type as a one-to-one VCC cell relay.                                                                                                                                                                                                                                                                        |
| <b>ignore-vpi-vci</b>                   | <p>Sets the Cisco MWR 2941 to ignore the VPI/VCI value in the PW packet and rewrite the egress ATM cell header with VPI/VCI value of the locally configured (attachment side) PVC.</p> <p>Note You can only use this parameter for a 1-to-1 pseudowire, for which you apply the xconnect command to a PVC.</p>                                                                                                                  |

**Command Default** The attachment circuit is not bound to the PW.

**Command Modes**

- CEM circuit configuration
- Interface configuration
- Subinterface configuration

l2transport configuration (for ATM)

Connect configuration

Global configuration

#### Command History

| Release     | Modification                                                                                                                                                                   |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(23)S   | This command was introduced.                                                                                                                                                   |
| 12.0(28)S   | Support was added for Multilink Frame Relay connections.                                                                                                                       |
| 12.3(2)T    | This command was integrated into Cisco IOS Release 12.3(2)T.                                                                                                                   |
| 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.                                                                                                                  |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC.                                                                                                                |
| 12.4(11)T   | This command was integrated into Cisco IOS Release 12.4(11)T.                                                                                                                  |
| 12.2(33)SRB | This command was updated to add support for AToM static pseudowires, and so that the remote router ID need not be the Label Distribution Protocol (LDP) router ID of the peer. |
| 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2.                                                                                                                |
| 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA.                                                                                                                |
| 12.2(33)MRB | The <b>manual</b> keyword was added.                                                                                                                                           |

#### Usage Guidelines

The **xconnect** command allows provisioning an AToM static pseudowire. Use the **manual** keyword in the **xconnect** command to place the router in xconnect configuration mode. MPLS pseudowire labels are configured using the **mpls label** and (optionally) **mpls control-word** commands in xconnect configuration mode.

The combination of the *peer-ip-address* and *vcid* arguments must be unique on the router. Each xconnect configuration must have a unique combination of *peer-ip-address* and *vcid* configuration.

The same *vcid* value that identifies the attachment circuit must be configured using the **xconnect** command on the local and remote PE routers. The *vcid* argument creates the binding between a PW and an attachment circuit.

The use of the **xconnect** command and the interface configuration mode bridge-group commands is not supported on the same physical interface.



#### Note

If the remote router is a Cisco 12000 series Internet router, the *peer-ip-address* argument must specify a loopback address on that router.

The **pw-class** keyword with the *pw-class-name* value binds the xconnect configuration of an attachment circuit to a specific pseudowire class. In this way, the pseudowire class configuration serves as a template that contains settings used by all attachment circuits bound to it with the **xconnect** command.



#### Note

If you specify the encapsulation keywords, you must specify the **pw-class** keyword.

#### ignore-vpi-vci Keyword

Using the **xconnect** command with the **ignore-vpi-vci** keyword provides benefits over using the pw-pvc command for PVC mapping.

Originally, PVC mapping was done through the **pw-pvc pw-vpi/pw-vci** command. When the MWR received the MPLS PW packet, it decoded the PW payload and looked up the PW VPI/VCI value to see if it matched any local configured PVC values. If a match was made, the PW-VPI/PW-VCI was translated to the AC-side VPI/VCI and the cell was sent to the local PVC. Without a match, the MWR dropped the received PW packet. When the MWR generated the PW packet, it used configured **pw-vpi/pw-vci** values. In this case, the PVC mapping was done completely on the MWR and was transparent to the remote end.

The process changes when the **ignore-vpi-vci** keyword is configured. For N:1 with N=1 special case, when the PW packet is received from the MWR, the receiving router ignores the VPI/VCI value contained in the PW payload. It does a blind rewrite to use the AC-side VPI/VCI and sends the cell to the AC side PVC.

The **xconnect** command with the **ignore-vpi-vci** keyword results in the PVC mapping being done in a cooperative way if the MWR works the same way as the receiving router. Without this command, the MWR checks the VPI/VCI value inside the PW packet for matches against the local configured PVC or PVC-mapping. With the **ignore-vpi-vci** keyword configured, the MWR ignores the VPI/VCI header inside the received PW packet and does a blind rewrite with the local configured AC-side PVC's VPI/VCI value. This process applies only to N:1 VCC PW with N=1 special case.

## Examples

The following example configures **xconnect** service for an ATM interface by binding the ATM circuit to the PW named 123 with a remote peer 10.0.3.201. The configuration settings in the pseudowire class named ATM-xconnect are used.

```
Router# config tby
Router(config)# interface ATM 0/0
Router(config-if)# xconnect 10.0.3.201 123 pw-class ATM-xconnect
Router(config-if-xconn)# exit
Router(config-if)# exit
Router(config)# exit
```

The following example illustrates PVC mapping using the **ignore-vpi-vci** keyword with the **xconnect** command. The example shows both the MWR and remote end (7600) routers.

MWR:

```
Router# config t
Router(config)# interface ATM 0/0
Router(config-if)# pvc 0/10 12transport
Router(config-if-atm-12trans-pvc)# encapsulation aa10
Router(config-if-atm-12trans-pvc)# xconnect 10.10.10.10 100 encapsulation mpls ignore-vpi-vci
Router(config-if-atm-12trans-pvc-xconn)# exit
Router(config-if-atm-12trans-pvc)# exit
Router(config-if)# exit
Router(config)# exit
```

7600:

```
Router# config t
Router(config)# interface ATM 0/0
Router(config-if)# pvc 2/20 12transport
Router(config-if-atm-12trans-pvc)# encapsulation aa10
Router(config-if-atm-12trans-pvc)# xconnect 20.20.20.20 100 encapsulation mpls
Router(config-if-atm-12trans-pvc-xconn)# exit
Router(config-if-atm-12trans-pvc)# exit
Router(config-if)# exit
Router(config)# exit
```

| Related Commands | Command                 | Description                                                                                               |
|------------------|-------------------------|-----------------------------------------------------------------------------------------------------------|
|                  | <b>pseudowire-class</b> | Configures a template of PW configuration settings used by the attachment circuits transported over a PW. |
|                  | <b>show xconnect</b>    | Displays information about xconnect attachment circuits and PWs.                                          |

# xconnect logging redundancy

To enable system message log (syslog) reporting of the status of the xconnect redundancy group, use the **xconnect logging redundancy** command in global configuration mode. To disable syslog reporting of the status of the xconnect redundancy group, use the **no** form of this command.

**xconnect logging redundancy**

**no xconnect logging redundancy**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Syslog reporting of the status of the xconnect redundancy group is disabled.

**Command Modes** Global configuration

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.0(31)S   | This command was introduced.                                    |
|                 | 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.  |
|                 | 12.4(11)T   | This command was integrated into Cisco IOS Release 12.4(11)T.   |
|                 | 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
|                 | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |
|                 | 12.4(19)MR2 | This command was integrated into Cisco IOS Release 12.4(19)MR2. |
|                 | 12.2(33)MRA | This command was integrated into Cisco IOS Release 12.2(33)MRA. |

**Usage Guidelines** Use this command to enable syslog reporting of the status of the xconnect redundancy group.

**Examples** The following example enables syslog reporting of the status of the xconnect redundancy group and shows the messages that are generated during switchover events:

```
Router# config t
Router(config)# xconnect logging redundancy
Router(config)# exit
```

**Activating the Primary Member**

```
00:01:07: %XCONNECT-5-REDUNDANCY: Activating primary member 10.55.55.2:1000
```

**Activating the Backup Member:**

```
00:01:05: %XCONNECT-5-REDUNDANCY: Activating secondary member 10.55.55.3:1001
```

| Related Commands | Command  | Description                                                                                                                                     |
|------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | xconnect | Binds an Ethernet, 802.1q VLAN, or Frame Relay attachment circuit to an Layer 2 PW for xconnect service and enters xconnect configuration mode. |





## INDEX

---

### A

ATM port [4-6](#)  
attachment circuits [1-3](#)  
autodiscovery [4-46](#)  
auxiliary port [3-2](#)

---

### B

base station controller  
    *See* BSC  
base station controller (BSC) [4-6](#)  
base transceiver station  
    *See* BTS  
before starting router [3-3](#)  
BSC  
    in RAN [1-1](#)  
BTS  
    in RAN [1-1](#)

---

### C

circuit emulation service over packet-switched network [1-3](#)  
Cisco IOS  
    about [2-1](#)  
    command modes [2-1](#)  
    enable mode [2-2, 4-46](#)  
    help [2-1](#)  
    saving configuration changes [2-3](#)  
    undo command [2-2](#)  
    undo feature [2-2](#)  
    configuration statements [1-7](#)

Cisco MWR 2941-DC router  
    monitoring and managing [4-46](#)  
    port numbering [3-2](#)  
    show commands for monitoring [4-48](#)  
    slot numbering [3-2](#)  
    understanding interface numbering [3-1](#)  
Cisco Pseudowire Emulation Edge-to-Edge  
    *See* PWE3  
Cisco pseudowire emulation edge-to-edge  
    *See* PWE3  
clocking  
    clocking example (figure) [4-6](#)  
clock signal [4-6](#)  
command line interface  
    *See* CLI  
command modes  
    global configuration [2-2](#)  
    interface configuration [2-2](#)  
    privileged EXEC [2-2](#)  
    user EXEC [2-2](#)  
commands  
    backup delay [A-4](#)  
    backup peer [A-6](#)  
    boot [3-4](#)  
    cdp enable [A-8](#)  
    cem-group [A-9](#)  
    class cem [A-11](#)  
    clear gsm-abis [A-13](#)  
    copy running-config [2-3](#)  
    dejitter-buffer [A-15](#)  
    gsm-abis congestion abate [A-16](#)  
    gsm-abis congestion critical [A-17](#)  
    help [2-1](#)

idle-pattern [A-27](#)  
 ima-group [A-28](#)  
 interface atm ima [A-29](#)  
 ip local interface [A-30](#)  
 keepalive [A-45](#)  
 load-interval [A-47](#)  
 match ip dscp [A-49](#)  
 mpls ip [A-51, A-67, A-69, A-70](#)  
 pseudowire-class [A-59](#)  
 pw-pvc [A-77](#)  
 sample-rate [A-57](#)  
 setup [3-3](#)  
 show atm cell-packing [A-81](#)  
 show cem circuit [A-82](#)  
 show cem platform [A-84](#)  
 show connection [A-86](#)  
 show controller [A-88](#)  
 show gsm-abis efficiency [A-90](#)  
 show gsm-abis errors [A-93](#)  
 show gsm-abis packets [A-95](#)  
 show gsm-abis peering [A-96](#)  
 show gsm-abis traffic [A-98](#)  
 show mpls l2transport vc [A-102](#)  
 show version [4-1](#)  
 show xconnect all [A-114](#)  
 snmp-server enable traps ipran [A-117](#)  
 snmp-server enable traps ipran alarm-gsm [A-118](#)  
 snmp-server enable traps ipran util [A-119](#)  
 undo [2-2](#)  
 xconnect [A-121](#)  
 xconnect logging redundancy [A-124](#)  
 configuration  
   before starting router [3-3](#)  
   completing [3-6](#)  
   first-time [3-1](#)  
   saving [2-3, 3-6, 4-45](#)  
 configuration statements for  
 CISCO-IP-RAN-BACKHAUL-MIB [1-7](#)  
 configuring

controllers  
   E1 interface [4-23](#)  
   for SNMP support [4-33](#)  
   GE interfaces [4-4](#)  
   global parameters [3-3](#)  
   gsm-abis congestion critical [A-17](#)  
   gsm-abis congestion onset [A-19](#)  
   gsm-abis jitter [A-20](#)  
   GSM-Abis links [4-31](#)  
   gsm-abis local [A-22](#)  
   gsm-abis remote [A-24](#)  
   hostname [4-2](#)  
   IP address [4-4](#)  
   multilink interface [4-22](#)  
   password [4-2](#)  
 console port [3-2](#)  
 controllers  
   E1 configuration [4-23](#)

---

## D

data bearer traffic [1-6](#)  
 duplex mode, setting [4-5](#)

---

## E

E1 controllers [4-23](#)  
 enable mode [2-2, 4-46](#)  
 event monitoring [4-46](#)

---

## F

figure  
   asymmetric PWE3 configuration [B-2](#)  
   ATM over MPLS configuration [B-25](#)  
   Cisco MWR 2941-DC router in a cell site POP [1-6](#)  
   Cisco MWR 2941-DC router in a PWE3 [1-2](#)  
   clocking example [4-6](#)

- GSM only configuration [B-32](#)
- GSM only configuration through satellite [B-36](#)
- PWE3 redundancy configuration [B-15](#)
- TDM over MPLS configuration [B-21](#)

first-time configuration [3-1](#)

## G

- GE interface
  - configuring [4-4](#)
  - IP address [4-4](#)
  - mode [4-5](#)
  - speed [4-5](#)
- global parameters
  - configuring [3-3](#)
- GSM Abis
  - example of Cisco MWR 2941-DC router in a GSM Abis Iub over IP (figure) [1-4](#)
- gsm-abis congestion abate
  - set [A-16](#)
- gsm-abis congestion critical
  - configure [A-17](#)
- gsm-abis congestion onset
  - configure [A-19](#)
- gsm-abis jitter
  - configure [A-20](#)
- GSM-Abis links
  - configuring [4-31](#)
- gsm-abis local
  - configure [A-22](#)
- gsm-abis remote
  - configure [A-24](#)

## H

- help, Cisco IOS [2-1](#)
- hostname
  - configuring [4-2](#)
  - verifying [4-3](#)

- intelligent cell site IP services [1-5](#)
- interface
  - configuring E1 [4-23](#)
  - GE, configuring [4-4](#)
  - multilink [4-22](#)
- IOS software
  - basics [2-1](#)
  - verifying version [4-1](#)
- IP address
  - configuring [4-4](#)
  - GE interface [4-4](#)

## M

- MIB support [1-11](#)
- mobile switching center
  - See* MSC
- monitoring and managing the Cisco MWR 2941-DC router [4-46](#)
- MSC
  - in a RAN [1-1](#)
- multilink interface
  - configuring [4-22](#)

## N

- Network-Clock-Participate [A-53](#)
- network-clock-select [A-53](#)

## P

- password [3-5](#)
  - configuring [4-2](#)
  - verifying [4-3](#)
- point-of-presence
  - See* POP
- POP

- cell site POP [1-5](#)
- example of Cisco MWR 2941-DC router in a cell site POP (figure) [1-6](#)
- port numbering
  - Cisco MWR 2941-DC router [3-2](#)
- provider edge [1-3](#)
- pseudowire-class [A-59](#)
- ptp announce [A-61](#)
- ptp clock-destination [A-64](#)
- ptp clock-source [A-63](#)
- ptp delay-req [A-65](#)
- ptp master [A-69](#)
- ptp mode [A-70](#)
- ptp priority1 [A-71](#)
- ptp slave [A-73](#)
- ptp sync [A-65](#), [A-74](#)
- ptp sync limit [A-76](#)
- PWE3
  - example of asymmetric PWE3 configuration [B-2](#)
  - example of Cisco MWR 2941-DC router in a PWE3 (figure) [1-2](#)
  - example of PWE3 redundancy configuration [B-15](#)
  - overview [1-2](#)

---

## R

- RAN, using the Cisco MWR 2941-DC router [1-1](#)
- recovered-clock slave [A-78](#)
- RNC
  - in a RAN [1-1](#)

---

## S

- SAToP [1-3](#)
- saving configuration changes [2-3](#), [4-45](#)
- security [4-46](#)
- serial port [4-6](#)
- set network-clocks [A-80](#)
- setup command facility [3-3](#)

- show atm cell-packing [A-81](#)
- show commands for monitoring the Cisco MWR 2941-DC router [4-48](#)
- show controller [A-88](#)
- show controller rtm [A-90](#)
- show interface switchport backup [A-99](#)
- show network-clocks [A-107](#)
- show platform hardware rtm [A-108](#)
- show ptp clock [A-109](#)
- show ptp foreign-master-record [A-110](#)
- show ptp parent [A-111](#)
- show ptp port [A-112](#)
- show ptp time-property [A-113](#)
- signaling traffic [1-6](#)
- slot numbering
  - Cisco MWR 2941-DC router [3-2](#)
- SNMP support
  - configuring [4-33](#)
- software
  - IOS basics [2-1](#)
  - verifying version [4-1](#)
- speed, setting [4-5](#)
- Structure-agnostic TDM over Packet [1-3](#)
- Structure-agnostic TDM over Packet (SaToP) [1-3](#)
- switchport backup interface [A-120](#)
- synchronized network operation [4-6](#)

---

## T

- transmit clock [4-6](#)

---

## U

- undo feature
  - Cisco IOS [2-2](#)

---

## V

- verifying

hostname [4-3](#)  
password [4-3](#)  
software version [4-1](#)  
version of Cisco IOS software [4-1](#)

---

## W

web-based reporting [4-46](#)

